

全国计算机技术与软件专业技术资格（水平）考试参考用书

网络工程师考试同步辅导
——考点串讲、真题详解与强化训练

工业和信息化部教育与考试中心 推荐

肖文 吴刚山 主编 / 吴敏 赵毅 副主编

第3版

清华大学出版社

全国计算机技术与软件专业技术资格(水平)考试参考用书

网络工程师考试同步辅导——考点串讲、真题详解与强化训练
(第3版)

肖　文　吴刚山　主　编
吴　敏　赵　毅　副主编

清华大学出版社
北　京

内 容 简 介

本书是按照最新颁布的全国计算机技术与软件专业技术资格(水平)考试大纲要求编写的考试用书。全书分为 14 章，内容包括：数据通信基础、广域通信网、局域网与城域网、无线通信网、网络互连与互联网、下一代互联网、网络安全、网络操作系统与应用服务器的配置、组网技术、网络管理、网络规划与设计、计算机基础知识、计算机专业英语和考前模拟卷等内容。1～11 章分为备考指南、考点串讲、真题详解和强化训练 4 个部分，以帮助读者明确考试要求，把握命题规律与特点，掌握考试要点和解题方法。后面两章提供了计算机专业英语和两套模拟试题，供考生进行考前实践。

本书紧扣考试大纲，具有应试导向准确、考试要点突出、真题分析详尽、针对性强等特点，非常适合参加网络工程师考试的考生使用，也可作为高等院校或培训班的教材。

图书在版编目(CIP)数据

网络工程师考试同步辅导：考点串讲、真题详解与强化训练/肖文，吴刚山主编. —3 版. —北京：清华大学出版社，2018
(全国计算机技术与软件专业技术资格(水平)考试参考用书)
ISBN 978-7-302-50866-3

Ⅰ. ①网…　Ⅱ. ①肖…　②吴…　Ⅲ. ①计算机网络—资格考试—自学参考资料　Ⅳ. ①TP393

中国版本图书馆 CIP 数据核字(2018)第 178589 号

责任编辑： 魏　莹　李玉萍
装帧设计： 常雪影
责任校对： 吴春华
责任印制： 董　瑾
出版发行： 清华大学出版社
网　　址：http://www.tup.com.cn, http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969, c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015, zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn, 010-62791865
印 装 者： 北京鑫海金澳胶印有限公司
经　　销： 全国新华书店
开　　本： 185mm×260mm　　**印　张：** 34　　**字　数：** 826 千字
版　　次： 2011 年 4 月第 1 版　2018 年 9 月第 3 版　　**印　次：** 2018 年 9 月第 1 次印刷
定　　价： 98.00 元

产品编号：070686-01

前　　言

全国计算机技术与软件专业技术资格(水平)考试是我国国家人力资源和社会保障部、工业和信息化部领导下的国家考试，其目的是科学、公正地对全国计算机与软件专业技术人员进行职业资格、专业技术资格认定以及专业技术水平测试。它自实施起至今已经历了 20 多年，其权威性和严肃性得到了社会及用人单位的广泛认同，并为推动我国信息产业特别是软件产业的发展和提高各类 IT 人才的素质培养做出了积极的贡献。

本书第 1 版自 2011 年、第 2 版自 2014 年出版以来，被众多考生选用为考试参考书，多次重印，深受广大考生好评。为了更好地服务于考生，引导考生尽快掌握计算机的先进技术，并顺利通过网络工程师考试，根据计算机新技术和网络新技术的发展，本书对第 2 版同名书进行修订。

本书具有如下特色。

(1) 全面揭示命题特点。通过分析研究最近几年的考题，统计出各章所占的分值和考点的分布情况，引导考生把握命题规律。

(2) 突出严谨性与实用性。按照最新考试大纲和《网络工程师教程(第五版)》编写，结构与官方教程同步，内容严谨，应试导向准确。

(3) 考点浓缩，重点突出。精心筛选考点，突出重点与难点，针对性强。同时对于考试中出现的而指定教材没有阐述的知识点进行了必要的补充。

(4) 例题典型，分析透彻。所选例题出自最新真题，内容权威，例题分析细致深入，解答准确完整，以帮助考生增强解题能力，突出实用性。

(5) 习题丰富，附有答案。每章都提供了一定数量的习题供考生自测，并配有参考答案与解析，有利于考生巩固所学知识，提高解题能力。

(6) 全真试题实战演练。提供了两套考前模拟试卷供考生考前进行实战演练。试题题型、考点分布、题目难度与真题相当，便于考生熟悉考试方法、试题形式，全面了解试题的深度和广度。

本书特别适合参加计算机技术与软件专业技术资格(水平)考试的考生使用，也可作为相应培训班的教材，以及大、中专院校师生的教学参考书。

本书由肖文、吴刚山担任主编，吴敏、赵毅担任副主编，参与本书组织、编写和资料收集的还有钟彩华、傅伟玉、高洁、李静、初耀军、袁琴、吴亚军、郭传奇、杨宏、周瑜龙、赵明、汤小燕、何光明等，在此一并表示感谢。同时本书在编写过程中，还参考了许多相关的书籍和资料，在此也对这些参考文献的作者表示感谢。

由于作者水平有限，书中难免存在错漏和不妥之处，敬请读者批评指正。

编　者

目　　录

第 1 章 数据通信基础

1.1 备考指南

1.1.1 考纲要求

根据考试大纲中相应的考核要求，在“数据通信基础”知识模块上，要求考生掌握以下方面的内容。

(1) 信道特性。

(2) 调制和编码，包括 ASK、FSK、PSK、QPSK、采样定理、PCM、编码。

(3) 传输技术，包括通信方式(单工/半双工/全双工、串行/并行)、差错控制、同步控制、多路复用。

(4) 传输介质，包括有线介质和无线介质。

(5) 线路连接设备，包括调制解调器、DSU 和 DCU。

(6) 物理层。

1.1.2 考点统计

“数据通信基础”知识模块在历次网络工程师考试试卷中出现的考核知识点及分值分布情况如表 1.1 所示。

表 1.1 历年考点统计表

年 份	题 号	知 识 点	分 值
2017 年 下半年	上午：11～17	调制方式和码元速率、E1 载波、网络传输介质	7 分
	下午：无	无	0 分

续表

年份	题号	知识点	分值
2017年上半年	上午：3、6、12～16	海明码、尼奎斯特采样定理、香农定理、4B/5B编码、码元速率	7分
	下午：无	无	0分
2016年下半年	上午：14～17、28	码元速率、E载波、CRC校验	5分
	下午：无	无	0分
2016年上半年	上午：14～17	码元速率、海明码、T载波	4分
	下午：无	无	0分
2015年下半年	上午：15～17	调制方式和码元速率、E载波	3分
	下午：无	无	0分
2015年上半年	上午：14、15	调制方式和码元速率、尼奎斯特采样定理	2分
	下午：无	无	0分
2014年下半年	上午：14～16	尼奎斯特采样定理、香农定理、调制方式和码元速率	3分
	下午：无	无	0分
2014年上半年	上午：13～15、34	海明码、数据速率	4分
	下午：无	无	0分
2013年下半年	上午：13～15	CRC校验、香农定理	6分
	下午：无	无	0分
2013年上半年	上午：12、16	尼奎斯特采样定理、异步通信模式、同步数字系列、CRC校验	4分
	下午：无	无	0分
2012年下半年	上午：15～17	PCM编码、异步通信模式、调制方式和码元速率	6分
	下午：无	无	0分
2012年上半年	上午：13～17	PCM编码、E载波和T载波、曼彻斯特编码、4B/5B编码	10分
	下午：无	无	0分

1.1.3 命题特点

纵观历年试卷，本章知识点是以选择题的形式出现在试卷中的。本章知识点在历次考试上午试卷中，所考查的题量大约为6道选择题，所占分值为6分(约占试卷总分值75分中的8%)；在下午试卷中没有相关考题。本章考题主要检验考生是否理解相关的理论知识点，考试难度较低。

1.2 考点串讲

1.2.1 信道特性

1.2.1.1 信道带宽

1. 模拟信道带宽

模拟信道的带宽如图1.1所示。信道带宽 $W=f_2-f_1$，其中，f_1 是信道能通过的最低频率，f_2 是信道能通过的最高频率，两者都是由信道的物理特征所决定的。为了使信号传输中的失

真小些，信道要有足够的带宽。

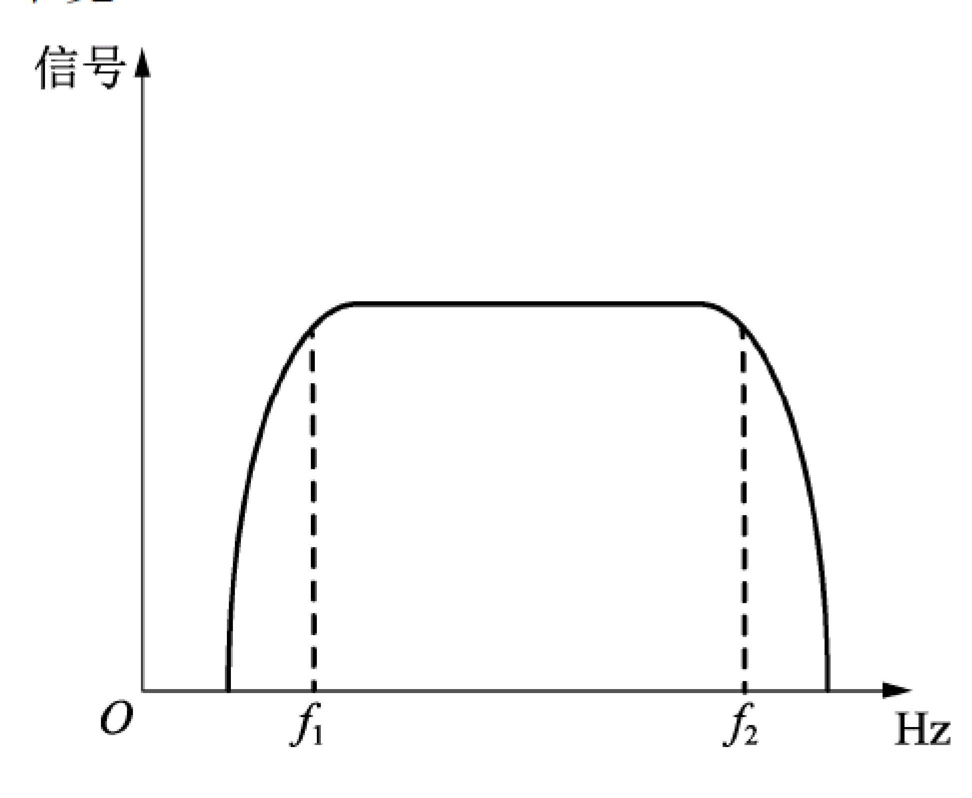


图 1.1　模拟信道的带宽

2. 码元、波特率、数据速率、数字信道带宽

一个数字脉冲称为一个码元，我们用码元速率表示单位时间内信号波形的变换次数，即单位时间内通过信道传输的码元个数。若信号码元宽度为 T 秒，则码元速率 $B=1/T$，其单位为波特。码元速率也称波特率。若一无噪声信道的带宽为 W，则该信道的极限波特率为 $B=2W$ (尼奎斯特定理)。码元携带的信息量 n (比特)与码元的种类数 N 的关系为 $n=\log_2 N$。

单位时间内在信道上传送的信息量(比特数)称为数据速率，其单位为比特。数据速率也称比特率。无噪声的信道的极限数据速率为 $R=B\log_2 N=2W\log_2 N$，其中，W 为信道带宽。有噪声的信道的极限数据速率为

$$C=W\log_2\left(1+\frac{S}{N}\right)\qquad(香农定理)$$

式中：W 为信道带宽；S 为信号的平均功率；N 为噪声平均功率；S/N 称为信噪比。

数字信道的带宽为信道能够达到的最大数据速率。数字信道的带宽和模拟信道的带宽可以通过香农定理互相转换。

1.2.1.2　误码率、信道延迟

误码率表示传输二进制位时出现差错的概率，其计算公式为 $P_c=N_e/N$。其中，N_e 为出错的位数，N 为传送的总位数。计算机通信一般要求误码率低于 10^{-6}，即平均 1 兆位错 1 位。

信号在信道中传播，从信源端到达信宿端需要的时间称为信道延迟。网络不同，信道延迟对该网络应用产生的影响也不同。

1.2.2　传输介质

1.2.2.1　双绞线

双绞线由粗约 1mm 的相互绝缘的一对铜导线绞扭在一起组成，对称均匀的绞扭可以减少线对之间的电磁干扰。双绞线大量应用在传统的电话系统中。双绞线分为屏蔽双绞线和非屏蔽双绞线。

1.2.2.2 同轴电缆

同轴电缆的芯线是铜质导线，外包一层绝缘材料，再外面是由细铜丝组成的网状导体，最外面加一层塑料保护膜，具有高带宽和较好的噪声抑制特性。局域网中常用的同轴电缆有两种：一种是特性阻抗为 50Ω，用于传输数字信号，叫作基带同轴电缆；另一种是特性阻抗为 75 Ω的 CATV 电缆，用于传输模拟信号，叫作宽带同轴电缆。

1.2.2.3 光纤

光纤由能传送光波的超细玻璃纤维制成，外包一层比玻璃折射率低的材料。进入光纤的光波在两种材料的界面上形成全反射，从而不断地向前传播。光纤分为多模光纤和单模光纤两种。在多模光纤中，光波以多种模式传播，不同的传播模式有不同的电磁场分布和不同的传播路径。在单模光纤中，光在其中无反射地沿直线传播。光纤的优点是具有很高的数据速率、极宽的频带、低误码率和低延迟，而且安全性和保密性好。

1.2.2.4 无线信道

微波通信系统可分为地面微波系统和卫星微波系统。微波通信的频段一般是 1～11GHz，具有带宽高、容量大、天线小、便于安装和移动的优点；缺点是容易受到电磁干扰，微波通信相互间也存在干扰，微波信号容易被大气层中的雨雪吸收。另外，在卫星微波系统中，信号时延也比较大。

红外传输系统利用墙壁或屋顶反射红外线，从而形成整个房间内的广播通信系统。其优点是设备相对便宜，带宽高；缺点是传输距离有限，且易受室内空气状态的影响。

无线电短波通信使用甚高频和超高频的电视广播频段。其优点是通信设备比较便宜，便于移动，没有方向性；缺点是容易受到电磁干扰和地形地貌的影响，而且带宽比微波通信小。

1.2.3 数据编码

数据编码的方式很多，主要有以下几种，其中几种如图 1.2 所示。

1. 单极性码

在这种编码方案中，只用正的(或负的)电压表示数据。在图 1.2 中用+3V 表示二进制数字 0，而用 0V 表示二进制数字 1。单极性码用在电传打字机(TTY)接口以及 PC 和 TTY 兼容的接口中，这种代码需要单独的时钟信号配合定时，它的抗噪声特性也不好。

2. 极性码

在这种编码方案中，分别用正电压和负电压表示二进制数 0 和 1。例如，在图 1.2 中用+3V 表示二进制数字 0，而用−3V 表示二进制数字 1。这种代码抗干扰特性好，但仍然需要另外的时钟信号。

3. 双极性码

在这种编码方案中，信号在 3 个电平(正、负、零)之间变化。一种典型的双极性码是信号交替反转编码(AMI)。在 AMI 信号中，数据流中遇到 1 时使电平在正和负之间交替翻转，而遇到 0 时则保持零电平。双极性是三进制信号编码方法，与二进制相比抗噪声特性更好。



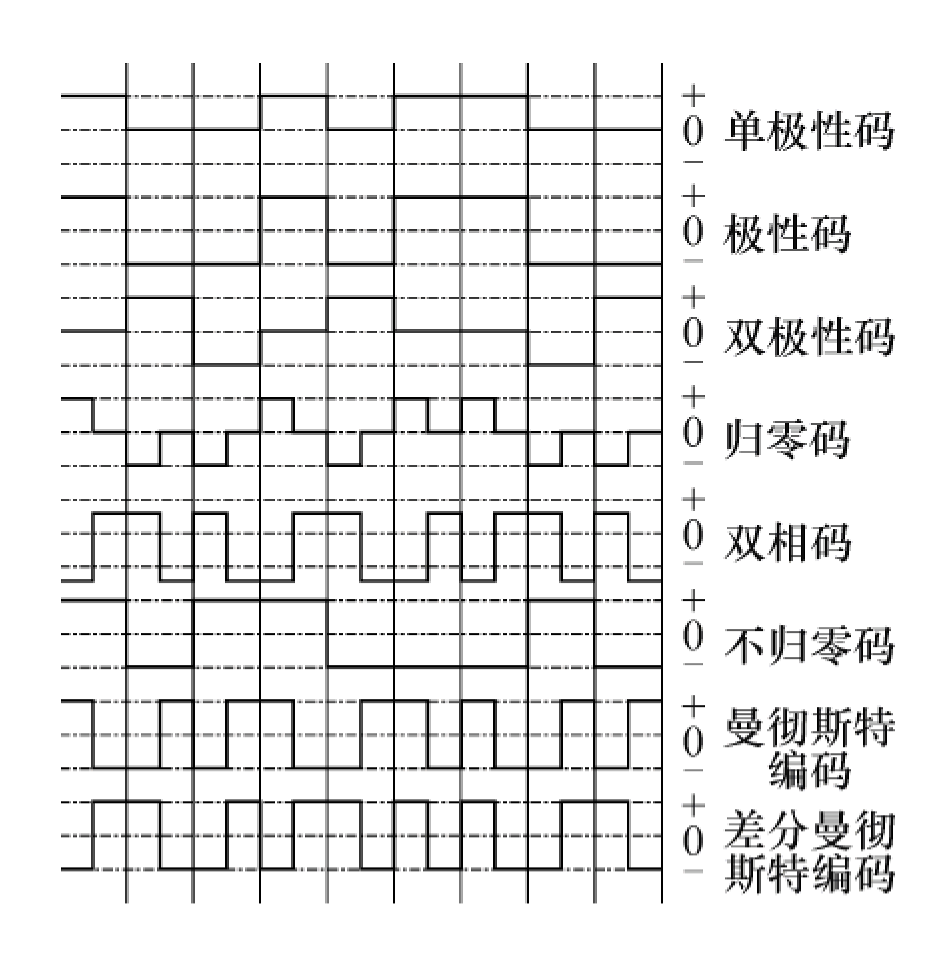


图 1.2　常用编码方案

4. 归零码

在归零码中，码元中间的信号回归到 0 电平，因此任意两个码元之间被 0 电平隔开。这种编码方案有较好的噪声抑制特性。图 1.2 中表示的是一种双极性归零码。可以看出，从正电平到零电平的转换边表示码元 0，而从负电平到零电平的转换边表示码元 1，同时每一位码元中间都有电平转换，从而使得这种编码成为自定时的编码。

5. 双相码

双相码要求每一位码元中都要有一个电平转换。这种代码是自定时的，同时也有检测错误的功能；如果某一位中间缺少了电平翻转，则被认为是错误代码。

6. 不归零码

图 1.2 中所示的不归零码的规律是当 1 出现时电平翻转，当 0 出现时电平不翻转。因而区别 1 和 0 的是电平是否翻转。这种代码也叫差分码，用在终端到调制解调器的接口中。这种代码不是自定时的。

7. 曼彻斯特编码

这种编码是一种双相码。图 1.2 中高电平到低电平的转换边表示 0，而用低电平到高电平的转换边表示 1，码元中间的电平转换边既表示数据代码，也作为定时信号使用。这种编码用在以太网中。

8. 差分曼彻斯特编码

这种编码也是一种双相码。这种编码的码元中间的电平转换边只作为定时信号，而不表示数据。数据的表示在于每一位开始处是否有电平转换：有电平转换表示 0，无电平转换表示 1。这种编码用在令牌环网中。

9. 多电平编码

这种编码的码元可取多个电平之一，每个码元可代表几个二进制位。例如，若表示码元的脉冲取 4 个电平之一，则一个码元可表示两个二进制位。

10. 4B/5B 编码

将欲发送的数据流每 4 位作为一个组，然后按照编码规则将其转换成相应的 5 位码。

该编码属于自同步编码方式，为了保证接收端能提取同步时钟，编码规则保证：无论4位数据为何种组合(包括全部为0)，所转换成5位码中至少有两个“1”，即保证在传输过程中码元至少发生两跳变，从而保证接收端同步时钟的提取。4B/5B编码能较好地解决同步问题，同时具有检错功能，编码效率比较高，它用5位信号表示4位有效信息，因此编码效率为80%。若要达到100 Mb/s的速率，只需在线路上有125 M的波特率。快速以太网(100Base-T)和光纤分布式接口(FDDI)都是采用4B/5B编码方式。

1.2.4 数字调制技术

数字数据在传输中不仅可以用方波脉冲表示，也可以用模拟信号来表示。数字调制是指用数字数据调制模拟信号。它主要有3种基本的调制方法：调幅、调频、调相。

1. 调幅

调幅(也称幅度键控ASK)，将不同的数据信息1和0调制成不同幅度但相同频率的载波信号。

2. 调频

调频(也称频移键控FSK)，将不同的数据信息1和0调制成相同幅度但不同频率的载波信号。

3. 调相

调相(也称相移键控PSK)，利用相邻载波信号的相位变化值来表示相邻信号是否具有相同的数据信息值，此时的幅度和频率均保持不变。

4. 正交调幅

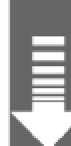
正交调幅(QAM)是一种十分成熟且应用广泛的调制技术。其基本方法是将发送数据流分为两路，分别对正弦载波和余弦载波进行数字调幅，然后相加传输。如果每路载波的幅度有n个不同幅度，则QAM信号的星座图上有n^2个状态点。这种方式的频谱利用率可以做得很高，设备也不太复杂。但是，当它的信号状态数很多时，则对信道的线性和非线性失真变得十分敏感，需要采用多种措施来对抗。

1.2.5 脉冲编码调制

脉冲编码调制(PCM)是一种数字化技术，用于将模拟数据变换为数字信号。变换的过程分为3个步骤：采样、量化和编码。

1. 采样

采样是指每隔一定时间间隔，取模拟信号的当前值作为样本，该样本代表了模拟信号在某一时刻的瞬时值。这样，就变连续的模拟信息为离散信号。采样技术依据尼奎斯特采样定理：如果采样速率大于模拟信号最高频率的两倍，则可以用得到的样本空间恢复原来的模拟信号。



2. 量化

量化的目的是确定采样出的模拟信号的数值。通过规定一定的量化级，对采样得到的模拟信号数值进行“取整”量化，从而得到离散信号的具体数值。量化级越高，表示离散信号的值精度越高。

3. 编码

编码是将量化后的样本值变成相应的二进制代码。通常，当量化级为 N 时，二进制位数为 $\log_2 N$。

例如，对声音数字化时，由于话音的最高频率是 4 kHz，所以采样速率是 8 kHz。对话音样本用 128 个等级量化，因而每个样本用 7 位二进制数字表示。在数字信道上传输的速率是 7×8000=56 Kb/s。

1.2.6　通信方式和交换方式

1.2.6.1　数据通信方式

1. 按通信方向分

按数据传输的方向分，数据通信有 3 种不同的通信方式：单工、半双工和全双工。

1)　单工

此方式下信道上的信息只能向一个方向传送，发送方不能接收，接收方也不能发送。例如，无线电广播和电视广播。

2)　半双工

此方式下通信的双方可交替发送和接收信息，但不能同时发送和接收。在一段时间内，信道的全部带宽用于一个方向上传送信息。例如，对讲机通信。

3)　全双工

此方式下可同时进行双向信息的传送，要求通信双方都有发送和接收设备。例如，电话通信。

2. 按同步方式分

在传送由多个码元组成的字符以及由许多字符组成的数据块时，通信双方要就信息的起止时间取得一致。这种同步作用有两种不同的方式，也对应了两种不同的传输方式：同步传输和异步传输。

1)　同步传输

同步传输适合传输连续的数据块。在这种方式下，发送方在发送数据前先发送一串同步字符 SYNC；接收方只要检测到连续两个以上 SYNC 字符就确认已进入同步状态，准备接收信息。随后的传送过程中双方以同一频率工作(信号编码的定时作用也表现在这里)，直到传送完指示数据结束的控制字符。

2)　异步传输

异步传输即把各个字符分开传输，字符之间插入同步信息。这种方式也称起止式，即在字符的前后分别插入起始位(“0”)和停止位(“1”)。起始位对接收方的时钟起置位作用。停止位告诉接收方该字符传送结束，然后接收方就可以检测后续字符的起始位。当没有字

符传送时，连续传送停止位。

1.2.6.2 交换方式

通信网络由许多交换节点互连而成，交换节点转发信息的方式可分为电路交换、报文交换和分组交换等。

1. 电路交换

这种交换方式用物理线路把发送方和接收方直接连通。类似于电话系统，此方式下的数据通信希望通信的计算机之间必须事先建立物理线路。整个电路交换的过程包括建立线路、占用线路并进行数据传输、释放线路 3 个阶段。

(1) 建立线路：发送方向接收方发送一个请求，该请求通过中间节点传输至终点，如果中间节点有空闲的物理线路可用，则接收请求，分配线路，并将请求传输给下一个中间节点。整个过程持续进行，直至终点。线路一旦被分配，在未释放之前，其他站点将无法使用。

(2) 数据传输：在已经建立的物理线路上，发送方和接收方进行数据传输。

(3) 释放线路：数据传输完毕后，执行释放线路的动作。线路被释放之后，进入空闲状态，可供其他站点通信使用。

电路交换的优点是独占性、实时性好，适合传输大量的数据。

2. 报文交换

报文交换也称存储—转发交换。这种方式不要求在两个通信节点之间建立专用线路。节点把要发送的信息组织成一个数据包——报文，该报文中含有目标节点的地址，完整的报文在网络中一站一站地向前传送。每一个节点接收整个报文，检查目标节点的地址，然后根据网络中的交通情况在适当的时候转发到下一个节点。经过多次的存储—转发，最后到达目标节点。其中的交换节点要有足够大的存储空间，用以缓冲收到的长报文。交换节点对各个方向上收到的报文排队，并寻找下一个转发节点，然后再转发出去，这些都带来了排队等待延迟。

报文交换的优点是不建立专用线路，线路利用率较高；缺点是有通信时延。

3. 分组交换

分组交换技术类似报文交换，只是它规定了交换设备处理和传输的数据长度(称为分组)。通常，分组的长度远小于报文交换中规定的报文长度。进行分组交换时，发送节点先对传送的信息分组，再对各个分组编号，加上源地址和目标地址以及约定的分组头信息。一次通信中的所有分组在网络中传播又有两种方式：数据报和虚电路。

1) 数据报

数据报类似于报文交换，每个分组都有完整的地址信息，不出意外的话，都可以到达目的地，但是到达顺序可能与发送顺序不一致，因此目标主机必须对收到的分组重新排序。这就需要在发送端有分组拆装设备对信息进行分组和编号，而在接收端需要分组拆装设备对收到的分组去头去尾并重新排序。数据报方式适合于单向地传送短消息。

2) 虚电路

虚电路类似于电路交换，要求在发送端和接收端之间建立一条逻辑连接，发送端发出的分组都走这一条通路，接收方要对正确收到的分组给予回答确认，直到会话结束，拆除



连接。逻辑连接的建立不意味着别的通信不能使用这条线路，仍然可以共享。虚电路适合于交互式通信。

1.2.7　多路复用技术

多路复用技术是把多个低速信道组合成一个高速信道的技术。这种技术要用到两个设备：多路复用器(Multiplexer)和多路分配器(Demultiplexer)。多路复用器，在发送端根据某种约定的规则把多个低带宽的信号复合成一个高带宽的信号；多路分配器，在接收端根据统一规则把高带宽信号分解成多个低带宽的信号。多路复用器和多路分配器统称为多路器，简写为 MUX。

多路复用技术主要分为 4 类：频分多路复用、时分多路复用、波分多路复用和码分多路复用。

1. 频分多路复用

频分多路复用(FDM)是在一条传输介质上使用多个频率不同的模拟载波信号进行多路传输。该技术对整个物理信道的可用带宽进行分割，利用载波调制技术实现原始信号的频谱迁移，使得多路信号在整个物理信道带宽允许的范围内实现频谱上的不重叠，从而共用一个信道。为了防止相互干扰，子信道间留有一定宽度的隔离频带。

2. 时分多路复用

时分多路复用(TDM)用于数字信道的复用。当物理信道可支持的位传输速率超过单个原始信号要求的数据传输速率时，可以将该物理信道划分成若干时间片，并将各个时间片轮流分配给多路信号，使得它们在时间上不重叠。时间片的宽度可以容纳一位、一个字节或一个固定大小的数据块。

3. 波分多路复用

波分多路复用(WDM)用在光纤通信中，不同的子信道用不同波长的光波承载，多路复用信道同时传送所有子信道的波长。因此，要使用能够对光波进行分解和合成的多路器。

4. 码分多路复用

码分多路复用(CDMA)也叫码分多址，是一种扩频多址的数字通信技术。在 CDMA 系统中，每个移动站都有相互正交的一个码片(Chip)，当发送码片序列表示 1，当发送码片序列的反码表示 0。其典型的应用是目前流行的 3G 技术。

5. 数字传输系统

1)　T1 载波

T1 载波在北美和日本广泛使用。它把 24 路按时分多路的原理复合在一条 1.544 Mb/s 的高速信道上。每路话音信道有 7 位数据位和一个信令位，周期为 125 μs，因此 24 路话音信道可容纳 8×24=192 位长的数字串。这 192 位数字组成一帧，最后再加入一个帧同步位，故帧长为 193 位。每 125 μs 传送一帧，这样，对每一路话音信道来说，传输数据的速率为 7 b/125 μs=56 Kb/s，传输控制信息的速率为 1 b/125 μs=8 Kb/s，总的速率为 193 b/125 μs=1.544 Mb/s。

2)　E1 载波

E1 载波在北美和日本以外的国家中使用(欧洲标准)。国际电报电话咨询委员会(CCITT)

于1993年后改为ITU-T，建议了一种PCM传输标准，称为E1载波。该载波把一个时分复用帧(其长度 T=125 μs)共划分为32个相等的时隙，每个时隙8位，时隙的编号为CH0～CH31，其中时隙CH0用作帧同步，时隙CH16用来传送信令，其他30个时隙用作30个话路。E1信道的传输速率为：8×32 b÷125 μs =2.048 Mb/s。

E2载波由4个E1载波组成，数据速率为8.448 Mb/s；E3载波由4个E2载波组成，数据速率为34.368 Mb/s；E4载波由4个E3载波组成，数据速率为139.24 Mb/s；E5载波由4个E4载波组成，数据速率为565.148 Mb/s。

6. 同步数字系列

光纤线路的多路复用标准有两个：美国标准SONET和国际标准SDH。

1) 同步光纤网 SONET

SONET的各级时钟都来自一个非常精确的主时钟。SONET定义了同步传输的线路速率的等级结构，其传输速率以51.840 Mb/s为基础。此速率对于电信号称为第1级同步传送信号，即STS-1；对于光信号则称为第1级光载波，即OC-1。

2) 同步数字系列SDH

ITU-T以美国标准SONET为基础，制定出国际标准同步数字系列SDH。一般可认为SDH与SONET是同义词。SDH的基本速率为155.52 Mb/s，称为第1级同步传递模块(Synchronous Transfer Module)，即STM-1，相当于SONET体系中的OC-3速率。

1.2.8 差错控制

通信系统必须考虑如何发现和纠正信号传输中的差错。通信过程中出现的差错可大致分为两类：一类是由热噪声引起的随机错误；另一类是由冲击噪声引起的突发错误。这里介绍三种常用的差错控制技术。

1. 奇偶校验

奇偶校验是最常用的检错方法，包括水平奇偶校验码、垂直奇偶校验码和水平垂直奇偶校验码。

1) 水平奇偶校验码

水平奇偶校验码也称字符校验码，是在7单位的ASCII代码后增加一位，使码字中“1”的个数成奇数(奇校验)或偶数(偶校验)。经过传输后，如果其中一位出错，则接收端按同样的规则就能发现错误。CCITT规定，异步传输方式中采用偶校验，同步传输方式中采用奇校验。

2) 垂直奇偶校验码

垂直奇偶校验码也称组校验，它将被传输的信息进行分组，并排列为若干行和列。组中每个字符的相同位进行奇偶校验，最终产生由校验位形成的校验字符，并附加在信息分组之后传输。

3) 水平垂直奇偶校验码

水平垂直奇偶校验码也称方阵校验，是在水平校验的基础上实施垂直校验。此时，为了保证随后一位的正确填充，水平垂直奇偶校验应采用偶校验。

2. 海明码

1950 年，海明研究了用冗余数据位来检测和纠正代码差错的理论和方法。按照海明的理论，可以在数据代码上添加若干冗余位组成码字。码字之间的海明距离是一个码字要变成另一个码字时必须改变的最小位数。例如，7 单位 ASCII 码增加一位奇偶位成为 8 位的码字，这 128 个 8 位的码字之间的海明距离是 2。所以，当其中 1 位出错便能检测出来。两位出错时就变成另一个码字。如果任意码字之间的海明距离是 d，则所有少于等于 d−1 位的错误都可以检查出来，所有少于 d/2 位的错误都可以纠正。对于某种长度的错误串，要纠正它就要用比仅仅检测它多一倍的冗余位。

3. 循环冗余校验码

循环冗余校验码(CRC)是一种循环码，其特征是信息字段和校验字段的长度可以任意选定，在局域网中有广泛应用。

生成 CRC 码的基本原理是：任意一个由二进制位串组成的代码都可以和一个系数仅为 0 和 1 取值的多项式一一对应。例如：代码 1010111 对应的多项式为 $x^6+x^4+x^2+x+1$。

CRC 码集选择的原则是：若设码字长度为 N 位，信息字段为 K 位，校验字段为 R 位(N=K+R)，则对于 CRC 码集中的任一码字，存在且仅存在一个 R 次多项式 $g(x)$，使得

$$V(x)=A(x)g(x)=x^R m(x)+r(x)$$

其中：$m(x)$为 K 次信息多项式；$r(x)$为 R−1 次校验多项式。

$$g(x)=g_0+g_1x+g_2x^2+\cdots+g_Rx^R$$

通常将 $g(x)$称为生成多项式，即所有合法的码字都可以由 $g(x)$生成。数据通信的发送方通过指定的 $g(x)$产生 CRC 码字，接收方则通过该 $g(x)$来验证收到的 CRC 码字。根据信息字段和 $g(x)$来生成/验证 CRC 码字的过程可由硬件和软件两种方法来实现。

(1) 软件实现的方法借助于多项式除法。

(2) CRC 可以用移位寄存器实现，移位寄存器由 k 位组成，还有几个异或门和一条反馈回路。如图 1.3 所示的移位寄存器可以按 CCITT-CRC 标准生成 16 位的校验和。寄存器被初始化为 0，数据从右向左逐位输入。当一位从最左边移出寄存器时就通过反馈回路进入异或门和后继进来的位以及左移的位进行异或运算。当所有 m 位数据从右边输入完后再输入 k 个 0(本例中 k=16)。最后，当这一过程结束时，移位寄存器中就形成了校验和。k 位的校验和随在数据位后边发送，接收端可以按同样的过程计算校验和并与接收到的校验和进行比较，以检测传输中的差错。

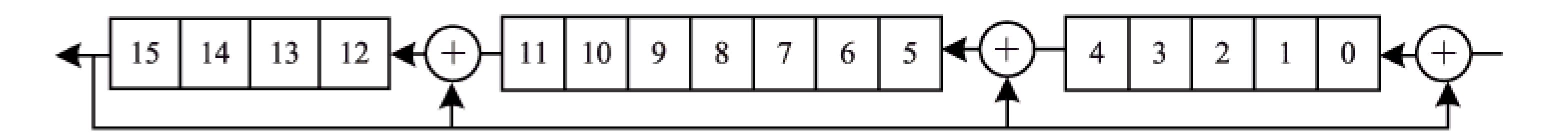


图 1.3　CRC 的实现

推荐的 CRC 生成多项式 $g(x)$为

CRC12=$x^{12}+x^{11}+x^3+x^2+x^1+1$　　R=12

CRC16=$x^{16}+x^{15}+x^2+1$　　R=16　　IBM 专用

CRC16=$x^{16}+x^{12}+x^5+1$　　R=16　　CCITT 专用

CRC32=$x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$　　R=32　LAN 中常用

1.3 真题详解

试题 1 (2017 年下半年试题 11 和试题 12)

图 1.4 所示的调制方式是 (11) ，若数据速率为 1Kb/s，则载波速率为 (12) Hz。

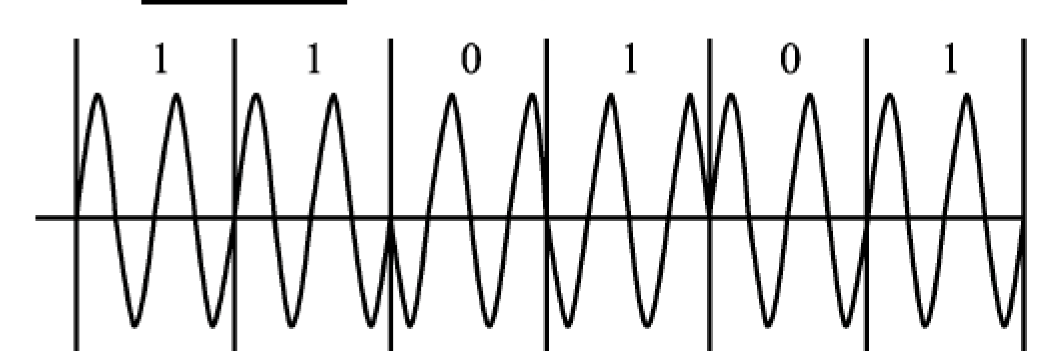


图 1.4 调制方式

(11) A. DPSK　　B. BPSK　　C. QPSK　　D. MPSK

(12) A. 1000　　B. 2000　　C. 4000　　D. 8000

参考答案：(11)A；(12)B。

要点解析：根据图形可知波形在 1 和 0 之间，以载波的相对初始相位变化来实现数据的传送，并且初始相位与前一码元发生 180 度变化为二进制 0，无变化为 1，可以判定为 DPSK(差分相移键控)。对应的码元速率和二进制数据速率相同，数据速率为 1Kb/s，因此载波频率为两倍。

试题 2 (2017 年下半年试题 13)

El 载波的子信道速率为 (13) Kb/s。

(13) A. 8　　B. 16　　C. 32　　D. 64

参考答案：(13)D。

要点解析：E1 载波的传输速率为 2.048Mb/s，每个子信道的速度是 64Kb/s。

试题 3 (2017 年下半年试题 14 和试题 15)

100Base-T4 采用的编码技术为 (14) ，利用 (15) 传输介质进行数据传输。

(14) A. 4B/5B　　B. 8B/6T　　C. 8B/10B　　D. MTL-3

(15) A. 光纤　　B. UTP-5　　C. UTP-3　　D. 同轴电缆

参考答案：(14)B；(15)C。

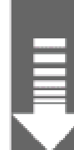
要点解析：100Base-T4 的信号采用 8B/6T 的编码方式，即每 8 位作为一组的数据转换为每 6 位一组的三元码组。其电缆类型为 4 对 3 类的非屏蔽双绞线，最大传送距离是 100 米。

试题 4 (2017 年下半年试题 16)

在异步通信中，每个字符包含 1 位起始位、8 位数据位、1 位奇偶位和 2 位终止位，若有效数据速率为 800b/s，采用 QPSK 调制，则码元速率为 (16) 波特。

(16) A. 600　　B. 800　　C. 1200　　D. 1600

参考答案：(16)A。



要点解析：每个字符的位数为 1+8+1+2=12，有效数据速率=标准速率×8/12=800b/s，则可得标准速率是 1200b/s。采用 QPSK 调制，那么码元速率×$\log_2 4$=1200，可得出码元速率为 600 波特。

试题 5 （2017 年下半年试题 17）

5 个 64Kb/s 的信道按统计时分多路复用在一条主线路上传输，主线路的开销为 4%，假定每个子信道利用率为 90%，那么这些信道在主线路上占用的带宽为 (17) Kb/s。

(17) A. 128　　B. 248　　C. 300　　D. 320

参考答案：(17)C。

要点解析：每个子信道利用率为 90%，因此有公式：5×64×90%=X×(1−4%)，解方程得 X=300。其中 5×64×90%=288Kb/s 为复用后速率。

试题 6 （2017 年上半年试题 3）

已知数据信息为 16 位，最少应附加 (3) 位校验位，才能实现海明码纠错。

(3) A. 3　　B. 4　　C. 5　　D. 6

参考答案：(3)C。

要点解析：海明码公式：$2^r > k+r+1$，其中 r 为校验位，k 为信息位数，由题意知信息位数为 16，显然 r 至少应为 5。

试题 7 （2017 年上半年试题 6）

数字语音的采样频率定义为 8kHz，这是因为 (6) 。

(6) A. 语音信号定义的频率最高值为 4kHz
　B. 语音信号定义的频率最高值为 8kHz
　C. 数字语音传输线路的带宽只有 8kHz
　D. 一般声卡的采样频率最高为每秒 8kHz

参考答案：(6)A。

要点解析：本题考查尼奎斯特取样定理：如果取样速率大于模拟信号最高频率的 2 倍，则可以用得到的样本空间恢复原来的模拟信号。因此采样频率=模拟信号频率×2，即模拟信号频率为一半 4kHz。

试题 8 （2017 年上半年试题 12 和试题 13）

电话信道的频率为 0～4kHz，若信噪比为 30dB，则信道容量为 (12) Kb/s，要达到此容量，至少需要 (13) 个信号状态。

(12) A. 4　　B. 20　　C. 40　　D. 80

(13) A. 4　　B. 8　　C. 16　　D. 32

参考答案：(12)C；(13)D。

要点解析：W(带宽)=4−0=4，由题可知 dB=10lg(S/N)=30，故 S/N=1000。

C(信道容量)=$W\times\log_2(1+S/N)=4\times\log_2 1001\approx 4\times\log_2 2^{10}=40$

$C=B\log_2 N=40$，又因 $B=2W=8$，所以 $N=32$。

试题 9 (2017 年上半年试题 14)

4B/5B 编码先将数据按 4 位分组，将每个分组映射到 5 单位的代码，然后采用__(14)__进行编码。

(14) A. PCM　　B. Manchester　　C. QAM　　D. NRZ-I

参考答案：(14)D。

要点解析：4B/5B 编码实际上是一种两级编码。系统中使用不归零编码，在发送到传输介质之前要变成见 1 就翻的不归零编码(NRZ-I)。NRZ-I 代码序列中 1 的个数越多，越能提供同步定时信息，但如果遇到长串的 0，则不能提供同步信息。所以在发送到介质之前还需要进行一次 4B/5B 编码，发送器扫描要发送的位序列，将其每 4 位分成一组，然后按照 4B/5B 编码规则转换成相应的 5 位代码。

试题 10 (2017 年上半年试题 15 和试题 16)

A、B 是局域网上两个相距 1km 的站点，A 采用同步传输方式以 1Mb/s 的速率向 B 发送长度为 200 000 字节的文件。假定数据帧长为 128 比特，其中首部为 48 比特，应答帧为 22 比特，A 在收到 B 的应答帧后发送下一帧。传送文件花费的时间为__(15)__s，有效的数据速率为__(16)__Mb/s(传播速率为 200m/μs)。

(15) A. 1.6　　B. 2.4　　C. 3.2　　D. 3.6

(16) A. 0.2　　B. 0.5　　C. 0.7　　D. 0.8

参考答案：(15)C；(16)B。

要点解析：总时间=传播时间+传输时间。

发送 200 000 字节，需要发送数据帧=(200 000×8)/(128−48)=20 000 个(数据帧)，那么应答帧=20 000 个。

传播时间=1000/200=5μs×40 000=0.2s。

传输时间=发送数据帧+发送应答帧时间。

发送一个数据帧时间：128/1 000 000。

发送一个应答帧时间：22/1 000 000。

所以，传输时间(150/1 000 000)×20 000=3s，则总时间=3.2s。

有效数据速率=(200 000×8)bit/3.2=0.5Mb/s。

试题 11 (2016 年下半年试题 14 和试题 15)

在异步通信中，每个字符包含 1 位起始位、7 位数据位、1 位奇偶位和 1 位终止位，每秒钟传送 100 个字符，采用 DPSK 调制，则码元速率为__(14)__，有效数据速率为__(15)__。

(14) A. 200 波特　　B. 500 波特　　C. 1000 波特　　D. 2000 波特

(15) A. 200b/s　　B. 500b/s　　C. 700b/s　　D. 1000b/s

参考答案：(14)C；(15)C。

要点解析：DPSK(差分相移键控)利用调制信号前后码元之间载波相对相位的变化来传递信息。码元速率=(1+7+1+1)×100=1000 波特，有效数据速率=[7/(1+7+1+1)]×1000=700b/s。

试题 12 (2016 年下半年试题 28)

在采用 CRC 校验时，若生成多项式为 $G(X)=X^5+X^2+X+1$，传输数据为 1011110010101



时，生成的帧检验序列为__(28)__。

(28) A. 10101　　B. 01101　　C. 00000　　D. 11100

参考答案：(28) C。

要点解析：CRC 循环冗余校验码利用循环码的误码检测特性进行误码检测，循环码的已编码字可被生成多项式 $g(X)$整除，接收端可以利用这一点进行检错，若不能整除，则有错。原始报文为 1011110010101，其生成多项式为：X^5+X^2+X+1，在原始报文后面添加 5 个 0(生成多项式的最高次幂为 5)作为被除数，除以生成多项式所对应的二进制数 100111，模除后得到的余数为校验码 00000。

试题 13　(2016 年上半年试题 14)

通过正交幅度调制技术把 ASK 和 PSK 两种调制模式结合起来组成 16 种不同的码元，这时数据速率是码元速率的__(14)__倍。

(14) A. 2　　B. 4　　C. 8　　D. 16

参考答案：(14)B。

要点解析：如果一个码元(取两个离散值)只携带 1 比特的信息量，则两者之间的数值相等；如果一个码元(取四个离散值)，则携带 2 比特的信息量。相关的换算公式为：$R=B\log_2 N$。

通过正交幅度调制技术把 ASK 和 PSK 两种调制模式结合起来组成 16 种不同的码元，故此时数据速率是码元速率的 4 倍。

试题 14　(2016 年上半年试题 15 和试题 16)

一对有效码字之间的海明距离是__(15)__。如果信息为 10 位，要求纠正 1 位错，按照海明编码规则，最少需要增加的校验位是__(16)__位。

(15) A. 两个码字的比特数之和　　B. 两个码字的比特数之差

C. 两个码字之间相同的位数　　D. 两个码字之间不同的位数

(16) A. 3　　B. 4　　C. 5　　D. 6

参考答案：(15)D；(16)B。

要点解析：码距就是两个码字 C1 和 C2 之间不同的比特数。例如：1100 与 1010 的码距为 2；1111 与 0000 的码距为 4。

校验码个数为 K，2 的 K 次方个校验信息，1 个校验信息用来指出“没有错误”，其余 $2k-1$ 个指出错误发生在哪一位，但也可能是校验位错误，所以满足 $m+k+1\leqslant 2k$。如果信息为 10 位，要求纠正 1 位错，按照海明编码规则，最少需要增加的校验位是 4 位。

试题 15　(2016 年上半年试题 17)

T1 载波的数据速率是__(17)__。

(17) A. 1.544Mb/s　　B. 6.312Mb/s　　C. 2.048Mb/s　　D. 44.736Mb/s

参考答案：(17)A。

要点解析：见表 1.2。

表 1.2

名　称	原理与组成	应用地区
T1 载波	采用同步时分复用技术将 24 个话音通路复合在一条 1.544Mb/s 的高速信道上	美国和日本
E1 载波	E1 的一个时分复用帧(其长度 T=125μs)共划分为 32 相等的时隙，时隙的编号为 CH0～CH31。其中 CH0 用作帧同步，CH16 用来传送信令，剩下 CH1～CH15 和 CH17～CH31 共 30 个时隙用作 30 个话路。每个时隙传送 8bit，因此共用 256bit。每秒传送 8000 个帧，因此 PCM 一次群 E1 的数据率就是 2.048Mb/s	欧洲发起，除美、日外多用
T2(DS2)	由 4 个 T1 时分复用而成，达到 6.312Mb/s	美国和日本
T3(DS3B)	由 7 个 T2 时分复用而成，达到 44.736Mb/s	美国和日本
T4(DS4B)	由 6 个 T3 时分复用而成，达到 274.176Mb/s	美国和日本

试题 16　(2015 年下半年试题 15)

设信号的波特率为 500Baud，采用幅度-相位复合调制技术，由 4 种幅度和 8 种相位组成 16 种码元，则信道的数据速率为__(15)__。

(15) A. 500 b/s　　B. 1000 b/s　　C. 2000 b/s　　D. 4800 b/s

参考答案：(15) C。

要点解析：数据传输速率 R 与波特率 B 之间的换算公式为：$R = B\log_2 N$。N 为码元的种类，本题为 16，因此 $R = 500 \times \log_2 16 = 500 \times 4 = 2000$ b/s。

试题 17　(2015 年上半年试题 14)

正交幅度调制 16-QAM 的数据速率是码元速率的__(14)__倍。

(14) A. 2　　B. 4　　C. 8　　D. 16

参考答案：(14) B。

要点解析：正交幅度调制形成了 16 种不同的码元，数据传输速率 R、码元速率 B、码元种类 N 之间的关系是：R=$B\log_2N$，因此 R=$B\log_2 16$=4B，可见数据速率是码元速率的 4 倍。

试题 18　(2015 年上半年试题 15)

电话线路使用的带通滤波器的带宽为 3kHz (300～3300Hz)，根据尼奎斯特采样定理，最小采样频率应为__(15)__。

(15) A. 300Hz　　B. 3390Hz　　C. 6000Hz　　D. 6600Hz

参考答案：(15) D。

要点解析：根据尼奎斯特采样定理，采样频率至少为最高频率的 2 倍。

1.4　强化训练

1.4.1　综合知识试题

试题 1　(2014 年下半年试题 14)

PCM 编码是把模拟信号数字化的过程，通常模拟话音信道的带宽是 4000Hz，则数字化



采样频率至少__(14)__次/秒。

(14) A. 2000　　B. 4000　　C. 8000　　D. 16000

试题 2　(2014 年下半年试题 15)

设信道带宽为 4000Hz，信噪比为 30dB，按照香农定理，信道容量为__(15)__。

(15) A. 4Kb/s　　B. 1.6Kb/s　　C. 40Kb/s　　D. 120Kb/s

试题 3　(2014 年下半年试题 16)

所谓正交幅度调制是把两个__(16)__的模拟信号合为一个载波信号。

(16) A. 幅度相同，相位相差 90 度　　B. 幅度相同，相位相差 180 度
C. 频率相同，相位相差 90 度　　D. 频率相同，相位相差 180 度

试题 4　(2014 年上半年试题 13)

地面上相距 2000km 的两地之间通过电缆传输 4000 比特长的数据包，数据速率为 64Kb/s，从开始发送到接收完成需要的时间为__(13)__。

(13) A. 48ms　　B. 640ms　　C. 32.5ms　　D. 72.5ms

试题 5　(2010 年下半年试题 14 和试题 15)

海明码是一种纠错的编码，一对有效码字之间的海明距离是__(14)__，如果信息为 6 位，要求纠正 1 位，按照海明编码规则，需要增加的校验位是__(15)__位。

(14) A. 两个码字的比特数之和
B. 两个码字的比特数之差
C. 两个码字之间相同的比特数
D. 两个码字之间不同的比特数

(15) A. 3　　B. 4　　C. 5　　D. 6

试题 6　(2010 年上半年试题 34)

假设网络的生产管理系统采用 B/S 工作方式，经常上网的用户数为 100 个，每个用户每分钟平均产生 11 个事务，平均事务量大小为 0.06MB，则这个系统需要的信息传输速率为__(34)__。

(34)A. 5.25Mb/s　　B. 8.8Mb/s　　C. 66Mb/s　　D. 528Mb/s

1.4.2　综合知识试题参考答案

【试题 1】答　案：(14)C。

解　析：根据 Nyquist 采样定律，编码时采样频率需至少为原始信号带宽的两倍，方可保证无损重建原始信号。

【试题 2】答　案：(15)C。

解　析：本题考察香农公式。香农公式为：$C=B\times\log_2(1+S/N)$，B 为宽带，S/N 为信噪比。而题干给出的信噪比为 dB，dB 和 S/N 的关系为：$dB=10\lg(S/N)$。30dB 时，可得出 S/N 为 1000。$C=B\times\log_2(1+S/N)=4000\times\log_2(1+1000)=40Kb/s$。

【试题 3】答　案：(16)A。

解　析：正交编码的两个信号源相位相差 90 度。

【试题 4】答　案：(13)D。

解　析：一个数据包从开始发送到接收完成的时间包含发送时间 t_f 和传播延迟时间 t_p 两部分，可以计算如下：对电缆信道 t_p=2000km/(200km/ms)=10ms，t_f=4000b/64000b/s=62.5ms，t_p+ t_f=72.5ms。

【试题 5】答　案：(14)D；(15)B。

解　析：海明码属于线性分组编码方式，大多数分组编码属于线性编码，其基本原理是，使信息码元与校验码元通过线性方程式联系起来。两个码字之间不同的比特数就是海明距离，此比特数又称为海明码距离。海明码的编码规则是：如果有 n 个数据位和 k 个冗余校验位，那么必须满足 $2k-1>n+k$，此处 k=4，因此有 $n≤2k-1-k$=16−1−4=11，n 最大为 11。

【试题 6】答　案：(34)B。

解　析：用户数量 100 个，每个用户每分钟产生 11 个事务，意味着这 100 个用户每秒可以产生(100×11)/6 个事务，每个事务量大小为 0.06MB，亦即每个事务量的比特数为 0.06MB×8=0.48Mbit。系统计算的信息传输速率单位是 b/s，(100×11×0.48)/60=8.8Mb/s。

第 2 章 广域通信网

2.1 备考指南

2.1.1 考纲要求

根据考试大纲中相应的考核要求，在“广域通信网”知识模块上，要求考生掌握以下方面的内容。

(1) 交换技术。

(2) 接入技术。

2.1.2 考点统计

“广域通信网”知识模块在历次网络工程师考试试卷中出现的考核知识点及分值分布情况如表 2.1 所示。

表 2.1 历年考点统计表

年 份	题 号	知 识 点	分 值
2017 年下半年	上午：18	帧中继、ATM	1 分
	下午：无	无	0 分
2017 年上半年	上午：17、18	光纤接入广域网	2 分
	下午：无	无	0 分
2016 年下半年	上午：12、50	PPP 协议、广域网的流量和差错控制	2 分
	下午：无	无	0 分
2016 年上半年	上午：18、67	XDSL	2 分
	下午：无	无	0 分

续表

年 份	题 号	知 识 点	分 值
2015 年下半年	上午：18、19、68、69	XDSL、HFC	4 分
	下午：无	无	0 分
2015 年上半年	上午：12、33	HDLC 协议、光纤接入网	2 分
	下午：无	无	0 分
2014 年下半年	上午：13、17～21	XDSL、ISDN、PPP 协议、帧中继网络	6 分
	下午：无	无	0 分
2014 年上半年	上午：58、59	移动 IP	2 分
	下午：无	无	0 分
2013 年下半年	上午：11、12	帧中继网络	4 分
	下午：无	无	0 分
2013 年上半年	上午：17	虚电路通信	2 分
	下午：无	无	0 分
2012 年下半年	上午：14	RS-232-C 标准	2 分
	下午：试题一	无线局域网接入技术	13 分
2012 年上半年	上午：13	帧中继	2 分
	下午：试题一	接入网技术	5 分

2.1.3 命题特点

纵观历年试卷，本章知识点是以选择题的形式出现在试卷中的。本章知识点在历次考试上午试卷中，所考查的题量为 3～4 道选择题，所占分值为 3～4 分 (占试卷总分值 75 分中的 4%～5%)；在下午试卷中较少出现，所考查的题量最多为 1 道综合案例题，所占分值大约为 15 分 (约占试卷总分值 75 分中的 20%)。大多数试题偏重于理论，考试难度中等。本章内容在最近几次考试中题量不固定，但总体来讲题量不多，教材改版后，题量有所增加。

X.25 公共数据网、帧中继网是重点考核内容。

ISDN、ATM 技术不是上午科目重点考查的内容，这部分内容在 2008 年之前经常出现在下午科目，不过最近几年很少考查。

2.2 考点串讲

2.2.1 公共交换电话网

公共交换电话网(Public Switched Telephone Network，PSTN)，从名称上就可以看出这是使用交换技术的网络。事实上，它正是以电路交换技术为基础的，用于传输模拟话音的网络。

电话网概括起来主要由 3 部分组成：本地回路、干线和交换机。其中，干线和交换机一般采用数字传输和交换技术，而本地回路(也称用户环路)基本上采用模拟线路。由于 PSTN

的本地回路是模拟的，因此当两台计算机想通过 PSTN 传输数据时，中间必须经双方 Modem(调制解调器)实现计算机数字信号与模拟信号的相互转换。

2.2.1.1　电话系统结构

如图 2.1 所示，用户电话通过一对铜线连接到最近的端局。而在应用于数字信号通信时，发送端把数字信号变换为模拟信号，接收端再把模拟信号变换为数字信号。局间干线则传输数字信号。

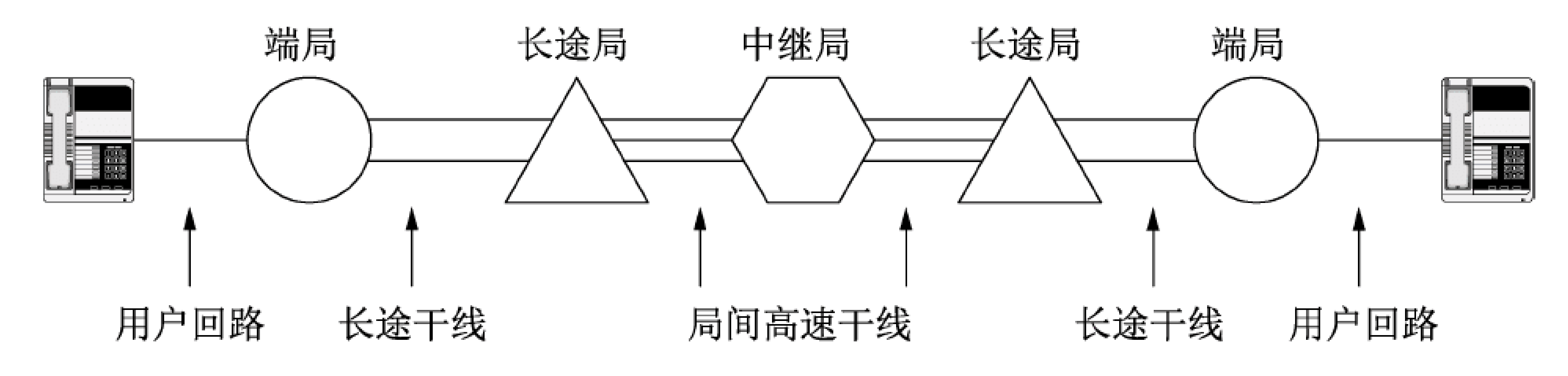


图 2.1　电话系统示意图

2.2.1.2　本地回路

用户把数据终端或计算机连接到电话网上就可进行通信。按照 CCITT 的术语，用户的数据终端或计算机叫作数据终端设备(DTE)。在通信网络一边，有一个设备管理网络的接口，这个设备叫数据电路设备(DCE)。DCE 通常指调制解调器等，提供建立、维持和拆除电路连接以及波形变换和编码的功能，如图 2.2 所示。

CCITT 和 ISO 用 4 个技术特性描述与设备之间通信有关的技术细节：机械特性、电气特性、功能特性和过程特性，具体如表 2.2 所示。

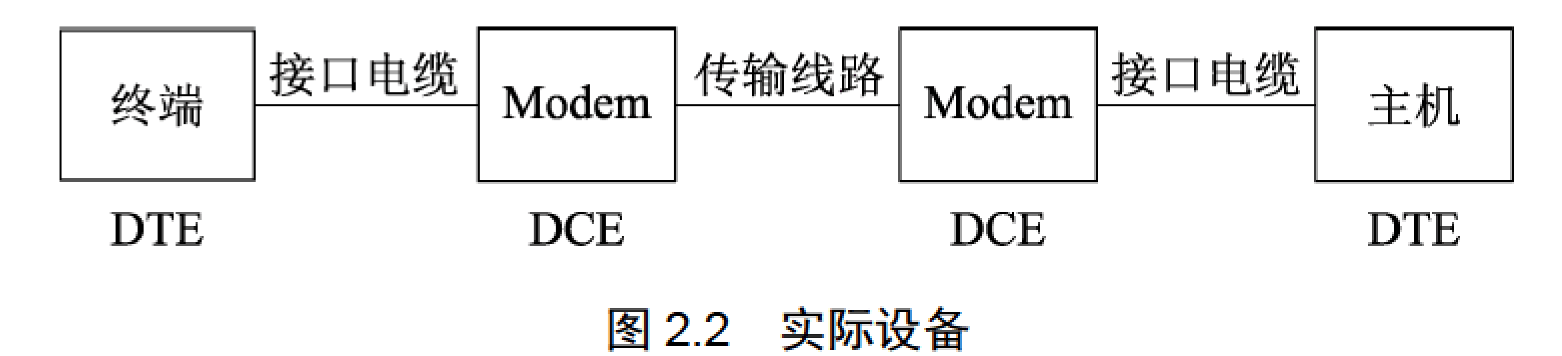


图 2.2　实际设备

表 2.2　CCITT 所描述的与 DTE/DCE 设备之间通信有关的技术特性

特　性	说　明
机械特性	描述了 DTE 和 DCE 之间物理上的分界线，规定连接器的几何形状、尺寸大小、引线数、引线排列方式以及锁定装置等。在微型机的 RS-232-C 串行接口上大多使用 9 针连接器
电气特性	RS-232-C 采用了 V.28 标准电路，信号源产生 3～15 V 的信号，±3 V 之间是信号电平过渡区，另外两种常用的电气特性标准是 V.10 和 V.11
功能特性	对接口连线的功能给出明确的定义。RS-232-C 采用的标准是 V.24。V.24 为 DTE/DCE 接口定义了 44 条连线，为 DTE/ACE 定义了 12 条连线。ACE 为自动呼叫设备。按照 V.24 的命名方法，DTE/DCE 连线用“1”开头的三位数字命名；DTE/ACE 连线用“2”开头的三位数字命名
过程特性	规定了使用接口线实现数据传输的操作过程

2.2.1.3　调制解调器

调制解调器(Modem)通常由电源、发送电路和接收电路组成。发送电路包括调制器、放

大器以及滤波、整形和信号控制电路，它的功能是把计算机产生的数字脉冲转换为已调制的模拟信号；接收电路包括解调器以及有关的电路，它的作用是把模拟信号变成计算机能接收的数字脉冲。

早期的低速 Modem 采用调频技术。后来的 Modem 采用四进制调相技术，即 2 比特对应一个相移，也有的 Modem 采用差分相移键控(DPSK)技术。

符合 CCITT V.29 建议的 Modem 以 9600 b/s 的速率进行全双工或半双工传输，并且采用正交幅度调制(QAM)技术。QAM 是每个 4 比特组的第一位，用于确定码元的幅度，而其余三位用于确定码元的相位。4 种幅度和 8 种相位的结合产生了 16 种不同的码元，因而在 2400 的波特率下可得到 9600 b/s 的数据速率。

符合 CCITT V.32 建议的 Modem 使用网格编码调制(TCM)技术。TCM 在 QAM 的基础上，在编码的过程中插入一个冗余比特，这个冗余比特根据卷积码的原理计算。接收端利用冗余比特进行纠错，从而减小误码率。调制器的输入数据流被分成 4 位的比特组，4 位的比特组经过卷积编码产生了第 5 位——冗余校验位。这种 Modem 可以在公共交换网上实现 9600 b/s 的高速传输。

符合 CCITT V.33 建议的 Modem 对 6 比特组进行幅度相位编码，再增加一个冗余位，形成 7 比特网络编码。在 2400 波特率下可达到 14 400 b/s 的数据速率。

符合 V.90 建议的 Modem 数据速率可达 56 Kb/s。这种 Modem 采用非对称的工作方式，从客户端向服务器端发送称为上行信道，数据速率为 28.8 Kb/s 或 32.6 Kb/s；从服务器端向客户端发送称为下行信道，数据速率可以达到 56 Kb/s。

2.2.2 X.25 公用数据网

X.25 是在 20 世纪 70 年代由国际电报电话咨询委员会制定的，其正式名称是“工作在公用数据网上以分组方式工作的数据终端设备 DTE 和数据电路设备 DCE 之间的接口”。1976 年 3 月 X.25 正式成为国际标准，后来又经过多次修订。在交换技术上，X.25 使用的是分组交换，因此它也常常被称为“X.25 分组交换网”。

X.25 标准分为 3 个协议层：物理层、链路层和分组层。它们分别对应于 OSI 参考模型底下三层。

- X.25 的物理层协议是 X.21，用于定义主机与物理网络之间物理、电气、功能以及过程特性。由于该标准要求用户在电话线路上使用数字信号，而不能使用模拟信号，所以实际上目前支持该物理层标准的公用网非常少，因为现在的电话线路大多数是使用模拟信号的。作为一个临时性措施，CCITT 定义了一个类似于大家熟悉的 RS-232 标准的模拟接口。
- X.25 的数据链路层描述用户主机与分组交换机之间数据的可靠传输，包括帧格式定义、差错控制等。X.25 数据链路层一般采用高级数据链路控制(High Level Data Link Control，HDLC)协议。事实上，它采用的是 HDLC 协议的一个部分——LAPB(平衡型链路接入规程)。
- X.25 的网络层描述主机与网络之间的相互作用，网络层协议处理诸如分组定义、寻址、流量控制以及拥塞控制等问题。网络层的主要功能是允许用户建立虚电路，然后在已建立的虚电路上发送最大长度为 128 个字节的数据报文。X.25 的分组层采用 PLP 协议。



2.2.2.1　CCITT X.21 标准

X.21 建议分为两部分：用于公共数据网同步传输的通用 DTE/DCE 接口和电路交换业务的呼叫控制过程。前者是 X.21 的物理层部分，与建立物理链路有关的操作过程有以下 4 个特性。

(1) 电气特性。X.21 采用 X.26 和 X.27 规定的两种接口电路。X.21 建议指定的数据速率有 600 b/s、2 400 b/s、4 800 b/s、9 600 b/s 和 48 000 b/s。X.21 规定，在 DTE 一边只能采用 X.27 规定的平衡电气特性；在 DCE 一边，对于超过 9 600 b/s 的速率只能采用平衡电气特性，而 4 种低速率则可以选择平衡的或不平衡电气特性。

(2) 机械特性。X.21 的机械接口采用 15 针连接器。

(3) 功能特性。X.21 的接口线比 RS-232-C 大为减少，通过对功能进行编码，在少量电路上传输代表各种功能的字符来建立对公共数据网的连接。X.21 定义的全部互换电路如图 2.3 所示。

(4) 过程特性。数据传输的动态过程如图 2.4 所示。

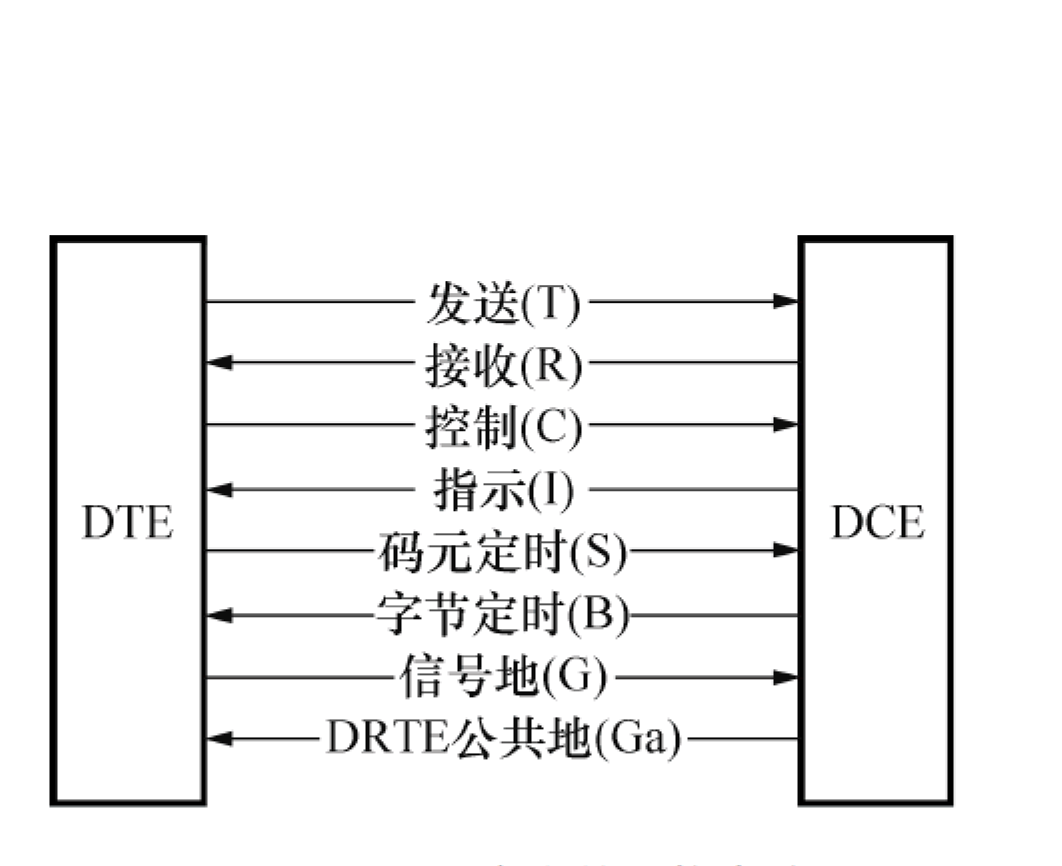


图 2.3　X.21 定义的互换电路

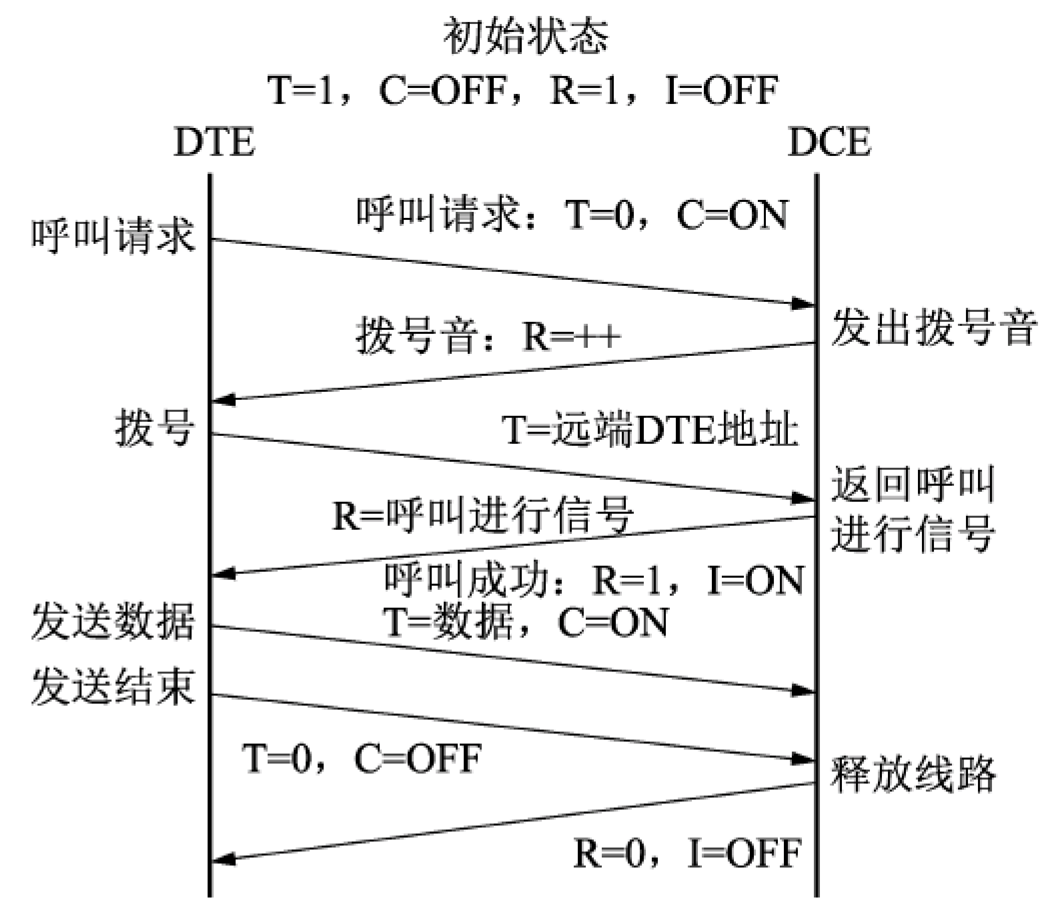


图 2.4　数据传输的动态过程

2.2.2.2　流量控制

流量控制是一种协调发送站和接收站工作步调的技术，其目的是避免发送速度过快，使得接收站来不及处理而丢失数据。

1. 停等协议

停等协议的工作原理是：发送站发出一帧，然后等待应答信号到达后再发送下一帧；接收站每收到一帧后送回一个应答信号(ACK)，表示愿意接收下一帧，如果接收站不送回应答信号，则发送站必须等待。

在半双工的点对点链路上，发送一帧的时间为：$T_{FA}=2t_p+t_f$。其中：t_p 为传播延迟；t_f 为发送一帧的时间(称为一帧时)。线路的利用率为

$$E=\frac{t_f}{2t_p+t_f} \tag{2.1}$$

定义 $a=t_p/t_f$，则

$$E=\frac{1}{2a+1} \tag{2.2}$$

线路传播延迟是线路长度 d 和信号传播速率 v 的比值，而一帧时是帧长 L 和数据速率 R 的比，因而有

$$a=\frac{d/v}{L/R}=\frac{Rd/v}{L} \tag{2.3}$$

2. 滑动窗口协议

滑动窗口协议的主要思想是允许连续发送多个帧，而无须等待应答。如果接收端维持能容纳 W 个帧的缓冲区(即窗口大小为 W)，那么发送端就可以连续发送 W 个帧而不必等待应答信号，但在收到接收端发送的确认之前，则发送端窗口不会移动。接收端收到一个帧时，就发送一个应答信号，并把窗口滑动到 i～W-i+1 的位置，表明 i 之前的帧已正确接收，期望接收后续的 W 个帧。随着数据传送过程的进展窗口向前滑动，因而取名滑动窗口协议。

滑动窗口协议的效率为：

$$E=\frac{W\times t_{\mathrm{f}}}{2t_{\mathrm{p}}+t_{\mathrm{f}}}=\frac{W}{2a+1} \tag{2.4}$$

3. 差错控制

利用差错检测技术自动地对丢失帧和错误帧请求重发的技术叫作 ARQ(Automatic Repeat reQuest)技术。

1) 停等 ARQ 协议

停等 ARQ 协议是停等流控技术和自动请求重发技术的结合。发送站发送一帧后必须等待应答信号，收到肯定应答信号 ACK 后继续发送下一帧；收到否定应答信号 NAK 后重发该帧；在一定的时间间隔内没有收到应答信号也必须重发。

2) 连续 ARQ 协议

连续 ARQ 协议是滑动窗口技术和自动请求重发技术的结合。由于窗口尺寸开到足够大时，帧在线路上可以连续地流动，因此又称其为连续 ARQ 协议。根据出错帧和丢失帧处理上的不同，连续 ARQ 协议又分选择重发 ARQ 协议和后退 N 帧 ARQ 协议。

选择重发 ARQ 协议只重发出错的帧，其后面的帧被缓存。采用 ARQ 协议时，窗口的最大值应为帧编号数的一半，即 $W_{发}=W_{收}\leqslant 2^{k-1}$。

后退 N 帧 ARQ 协议是从出错处重发已发过的 N 个帧。窗口的大小限制为 $W\leqslant 2^k-1$。

2.2.2.3 HDLC 协议

HDLC(High Level Data Link Control，高级数据链路控制)协议是国际标准化组织根据 IBM 公司的 SDLC 协议扩充开发而成的。它是一种面向位的数据链路控制协议。

HDLC 帧由 6 个字段组成，如图 2.5 所示。

(1) HDLC 用一种特殊的位模式 01111110 作为帧的边界标志。

(2) 地址字段用于标识从站的地址，用在点对多点链路中。

(3) HDLC 定义了 3 种帧：信息帧(I 帧)、管理帧(S 帧)和无编号帧(U 帧)，如图 2.6 所示。控制字段第 1 位或前两位用于区别 3 种不同格式的帧。基本的控制字段是 8 位长。扩展的控制字段为 16 位长。

(4) 信息字段只有 I 帧和某些无编号帧含有的信息字段。

(5) 帧校验序列通常使用 CRC-CCITT 标准产生的 16 位校验序列，有时也使用 CRC-32 产生的 32 位校验序列。



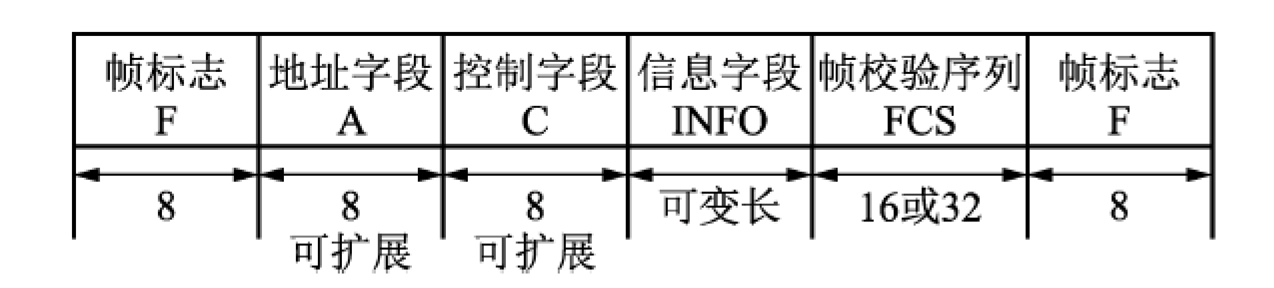


图 2.5　HDLC 帧结构

I帧	0	N(S)		P/F	N(R)
S帧	0	1	SS	P/F	N(R)
U帧	1	1	MM	P/F	MMM

图 2.6　HDLC 三种帧的基本控制信息

2.2.2.4　X.25 PLP 协议

1. 虚电路的建立和释放

X.25 的分组层提供虚电路服务。它支持交换虚电路(Switched Virtual Circuit，SVC)和永久虚电路(Permanent Virtual Circuit，PVC)。

- 交换虚电路是在发送方向网络发送请求建立连接报文要求与远程机器通信时建立的。一旦虚电路建立起来，就可以在建立的连接上发送数据，而且可以保证数据正确到达接收方。X.25 同时提供流量控制机制，以防止快速的发送方淹没慢速的接收方。SVC 的特点是灵活，当需要通信时才建立连接。但是，每次建立连接都会耗费时间。
- 永久虚电路的用法与 SVC 相同，但它是由用户和长途电信公司经过商议预先建立的，因而它时刻存在，用户不需要建立链路而直接使用它。PVC 有点类似于租用的专用线路。PVC 没有 SVC 那样灵活，但是它不需要花费时间建立连接，比较适用于需要及时通信的设备。

X.25 虚电路建立和释放的过程如图 2.7 所示。

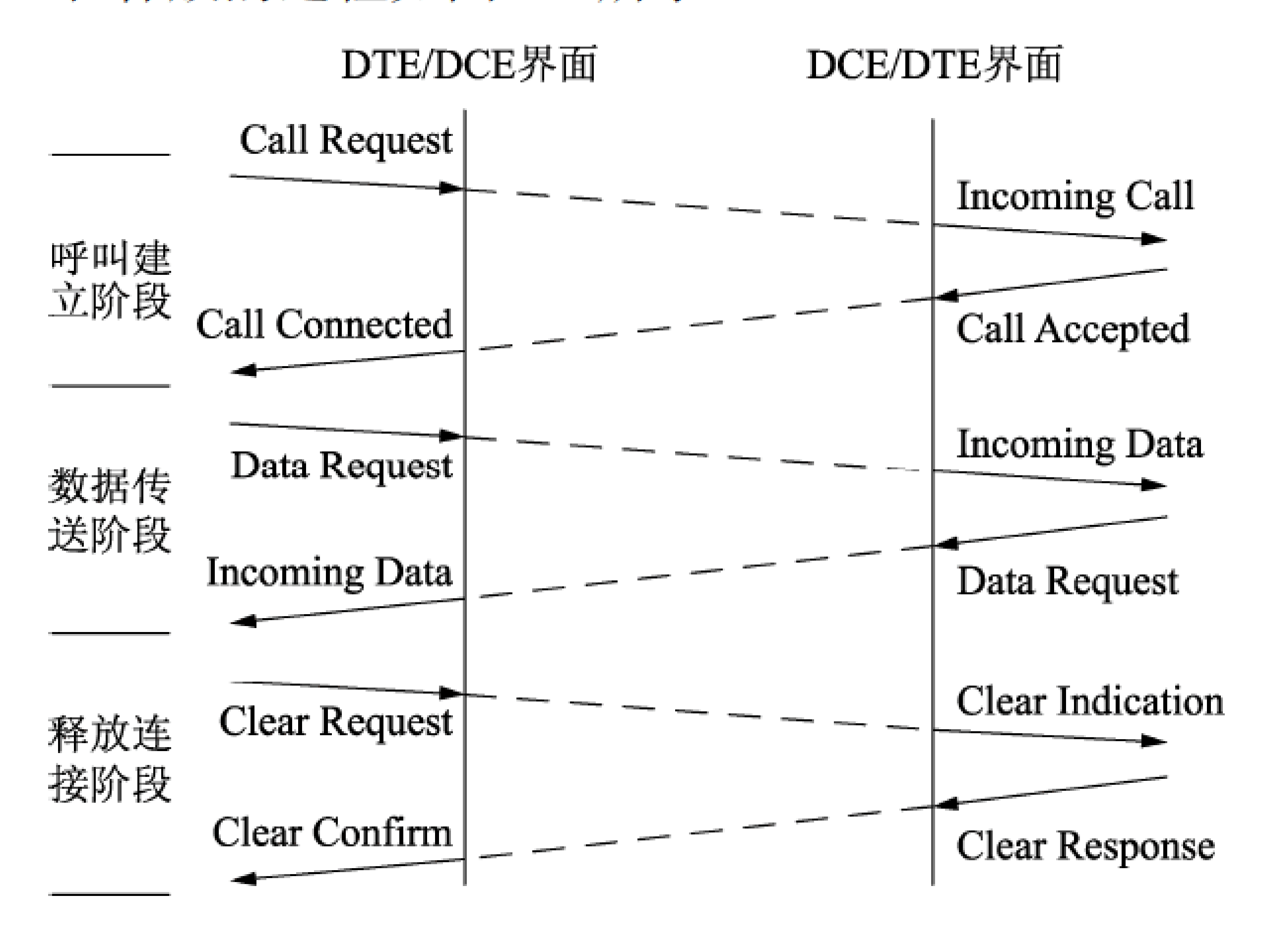


图 2.7　虚电路的建立和释放

2. PLP 协议

X.25 网络层采用分组级协议(Packet Level Protocol，PLP)。PLP 协议把用户数据分成一定大小的块(一般为 128 个字节)，再加 24 位或 32 位的分组头组成数据分组。分组头中第三个字节的最低位用来区分数据分组(该位为 0)和其他的控制分组(该位为 1)。

X.25 具有分组排序的功能，能识别分组组成的序列。当长的数据块经过一个只允许小分组通过的网络时，要保持数据块的完整性，就需要这个功能。

3. 流量和差错控制

X.25 的流量控制和差错控制机制与 HDLC 类似。X.25 默认的窗口大小是 2，但是对于 3 位顺序号，窗口最大可设置为 7；对 7 位的顺序号，窗口最大可设置为 127。这是在建立虚电路时通过协商决定的。X.25 的差错控制采用后退 *N* 帧 ARQ(自动重发请求)协议。

2.2.2.5 X.25 的优缺点

X.25 网络算是一个比较“古老”的网络了，它是在物理链路传输质量很差的情况下开发出来的。为了保障数据传输的可靠性，它在每一段链路上都要执行差错校验和出错重传。于是，X.25 的缺点很明显：由于复杂的差错校验机制导致了它的传输效率受到了限制。传输速率方面，X.25 网络并不是很快，它提供的数据传输速率一般为 64 Kb/s。

X.25 网络的优点如下。

- 可以在一条物理电路上同时开放多条虚电路供多个用户同时使用。
- 网络具有动态路由功能和复杂完备的误码纠错功能。
- X.25 分组交换网可以满足不同速率和不同型号的终端与计算机之间、计算机与计算机之间，以及局域网与局域网之间的数据通信。

2.2.3 帧中继网

帧中继技术是由 X.25 分组交换技术演变而来的，可以说是一种经过改进了的 X.25。与 X.25 一样，帧中继同样采用分组交换技术。然而，这种交换技术与通常的分组交换有些不同，有时也称这种分组交换为“快速分组交换”。

帧中继工作在 OSI 参考模型的底两层，即物理层和数据链路层。帧中继在第二层建立虚电路，用帧方式承载数据业务，因而第三层被简化掉了。同时 FR 的帧层比较简单，只做检错，不再重传，没有滑动窗口式的流控，只用拥塞控制。

2.2.3.1 帧中继服务

帧中继与 X.25 一样，也支持永久虚电路和交换虚电路，但是相对来说，永久虚电路使用得比较多一点。用户可以在两个节点之间租用一条永久虚电路，并通过该虚电路发送数据帧，其长度可达 1600 字节。用户也可以在多个节点之间通过租用多条永久虚电路进行通信。

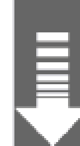
在帧中继的虚电路上可以提供不同的服务质量，服务质量参数如下。

- 接入速率(AR)：指 DTE 可获得的最大数据速率，即用户接入网络接口的物理速率。
- 约定突发量(Bc)：指在 Tc 时间间隔内允许用户发送的数据量。
- 超突发量(Be)：指在 Tc 时间间隔内超过 Bc 部分的数据流量。
- 约定数据速率(CIR)：指在数据通信过程中 ISP 能够保证的数据传输速率。
- 扩展数据速率(EIR)：指允许用户在 CIR 基础额外传输的数据速率。
- 约定速率测量时间(Tc)：指测量 Bc 和 Be 的时间间隔。
- 信息字段最大长度：指每个帧中包含的信息字段的最大字节数，默认为 1600 字节。

这些参数的关系为

$$Bc=Tc\times CIR$$
$$Be=Tc\times EIR$$





在帧中继网上，用户的数据速率可以在一定的范围内变化，从而既可以适应流式业务，又可以适应突发式业务，这使得帧中继成为远程传输的理想形式。

2.2.3.2　帧中继协议

帧中继协议叫作 D 信道链路接入规程(LAP-D)，它比平衡型链路接入规程(LAPB)简单，省去了控制字段。帧中继的帧格式如图 2.8 所示。LAP-D 帧头和帧尾都是一个字节的帧标志字段，编码为 01111110，信息字段长度可变，1600 字节是默认的最大长度。

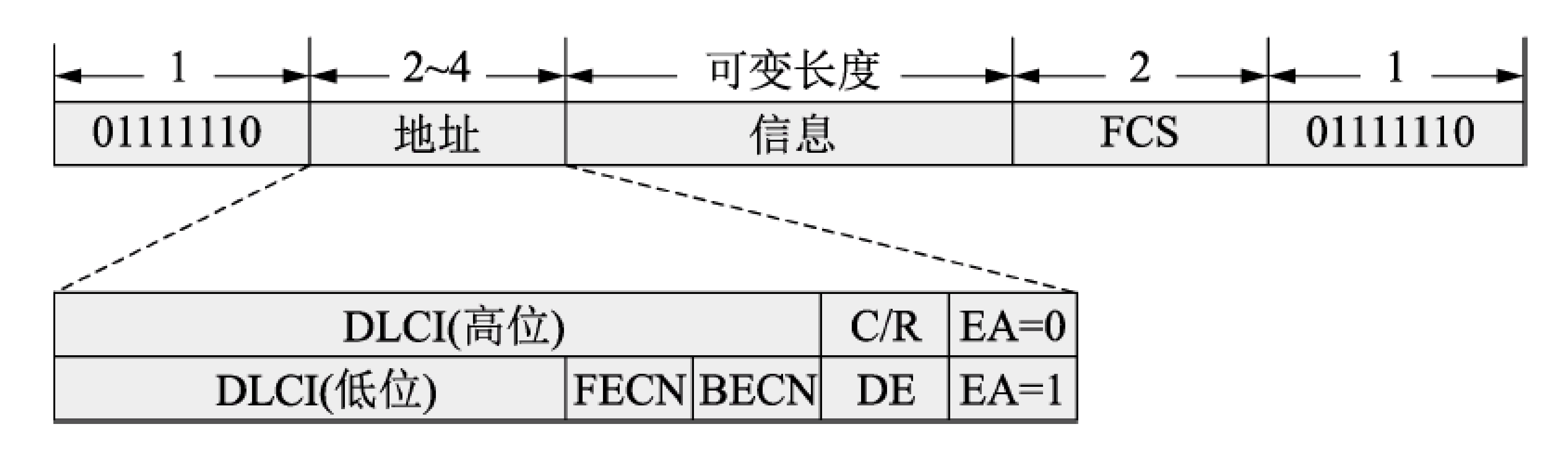


图 2.8　帧中继的帧格式

由于 LAP-D 增加了拥塞控制功能，所以帧格式中 FECN 位、BECN 位及 DE 位就显得比较重要。FECN 位是向前拥塞比特位，该位为 1 表示在传送方向上出现了拥塞，该帧到达接收方后，接收方可据此调整发送方的数据速率。BECN 位是向后拥塞比特位，该位为 1 表示在与传送相反的方向上出现了拥塞，该帧到达发送端后，发送方可据此调整发送数据的速率。DE 位是优先丢弃比特位，在网络发生拥塞时，DE 位为 1 的帧被优先丢弃。

2.2.3.3　帧中继的优点与应用

帧中继标准已渐成熟，业务需求不断增加，目前已进入高速发展时期。帧中继可通过 X.25 更新软件实现，也可在 DDN 网上配置端口来实现，在以 ATM 为主干的网络中，帧中继仍然可以作为良好的用户接入方式。

目前的路由器都支持帧中继协议，帧中继上可承载流行的 IP 业务，IP 加帧中继已经成了广域网应用的绝佳选择。近年来，帧中继上的话音传输技术(VOFR)也不断发展。

帧中继远程联网的主要优点如下。

- 基于分组(帧)交换的透明传输，可提供面向连接的服务。
- 帧长可变，长度可达 1600～4096 字节，可以承载各种局域网的数据帧。
- 数据速率可达 2M～45 Mb/s。
- 既可以按需要提供带宽，也可以应付突发的数据传输。
- 没有流控和重传机制，开销很少，传输效率高。

帧中继可以有效地处理突发性数据，当数据业务量为突发性时，由于帧中继具有动态分配带宽的功能，便允许用户的数据速率在一定范围内变化。但它不适于对延迟较敏感的应用(如音频、视频)，因为无法保证可靠地提交。

2.2.4　ISDN 和 ATM

2.2.4.1　ISDN

综合业务数字网(ISDN)是一种数字交换电话系统，它不仅支持电话网上的所有业务，

还能够提供数据透明传送业务和分组传送业务。ISDN 的中心思想是数字比特管道，它是客户和电信公司之间概念上的管道，比特流就从这里流过。在交换技术上，这种网络既支持线路交换也支持分组交换。

1. ISDN 系统结构

ISDN 的系统结构由 3 部分组成，分别是设备终端、网络终端和适配器。

设备终端(TE)有两种类型：TE1 和 TE2。前者可以和网络终端设备(NT)连接；后者被称为非 ISDN 设备，必须通过终端适配器(TA)才能把 TE2 连接到 NT 上面。

网络终端(NT)配置在用户端，通过用户端与网络端的交换设备相连接。为了满足不同的配置要求，NT 可以分为两种类型：NT1 和 NT2。

- NT1 是第一网络终端，被放置在用户设备和 ISDN 交换系统之间，不仅起到插板作用，还可以进行网络管理和维护等工作。
- NT2 具有交换和集线功能。
- TA 功能是把非 ISDN 的终端接入 ISDN 网络中。TA 的功能包括速率适配和协议转换等。

2. 两种 ISDN

ISDN 包括两种：窄带 ISDN 和宽带 ISDN。平常所说的 ISDN 就是窄带 ISDN(N-ISDN)，它是基于异步传输方式的技术。和 N-ISDN 一样，宽带 ISDN(B-ISDN)包括了 N-ISDN 的所有业务功能，它的主要任务就是以全新的交换体制来支持所有可能的电信业务。

ISDN 定义了一些标准化的通路，定义的标准如下。

- A 通路：4 kHz 带宽的标准模拟通路。
- B 通路：64 Kb/s 的数字脉码调制(PCM)话音或者数据通路。
- C 通路：8 Kb/s 或 16 Kb/s 的数字通路。
- D 通路：16 Kb/s 或 64 Kb/s 用作带外信令的数字通路。
- E 通路：64 Kb/s 的为内部 ISDN 信令使用的数字通路。
- H 通路：384 Kb/s、1358 Kb/s 或 1290 Kb/s 的数字通路。

另外，它还提供了两种标准的用户-网络接口，分别是基本速率接口和基群速率接口。基本速率接口允许用户使用模拟电话并且进行数据的纯数字通信，由两条 64 Kb/s 的 B 信道和一条 16 Kb/s 的 D 信道组成，合计的速率是 144 Kb/s。基群速率接口是指综合业务数字网(ISDN)中的一种用户—网络接口(UNI)，在该接口上，综合业务数字网(ISDN)向用户提供 30 个 B 信道(在 T1 中为 23 个)和一个 D 信道(信道速率为 64Kbit/s)。

1) 窄带 ISDN(N-ISDN)

N-ISDN 是一种基于电路交换网的技术，目的是以数字系统代替模拟电话系统，把音频、视频和数据业务在一个网络上一同传输。N-ISDN 以固定的比特速率向用户提供电路交换服务、分组服务和其他服务。

N-ISDN 系统提供两种用户接口：基本速率 2B+D 和一次群速率 30B+D。其中，B 信道是 64 Kb/s 的话音或数据信道，D 信道是 16 Kb/s 的信令信道。用户最多在 NT1 总线上挂接 8 台设备，共享 2B+D 的 144 Kb/s 信道。大型用户通过 NT2 接入 N-ISDN，享有 30B+D 达到 2.048 Mb/s 的速率。N-ISDN 采用的是时分多路复用技术。

N-ISDN 具有类似于 OSI 的三层结构。多路复用属于物理层的功能；ISDN 的数据链路



层采用 LAPD 协议；网络层主要支持电路交换和分组交换功能，与 X.25 的分组层协议极为相似。

N-ISDN 的缺点是数据传输速率太低，不适合视频信息等需要高带宽的应用。

2) 宽带 ISDN(B-ISDN)

B-ISDN 模型采用了与 OSI 同样的分层概念，同时还以不同的平面来区分用户信息、控制信息和管理信息。用户平面提供与用户数据传送有关的流量控制和差错检测功能；控制平面主要用于连接和信令信息的管理；管理平面支持网络管理和维护功能。

B-ISDN 的关键技术是异步传输模式(ATM)，采用五类双绞线或光纤传输，数据速率可达 155 Mb/s。

2.2.4.2　同步传输和异步传输

1. 同步传输模式

同步传输模式(STM)：在同步时分多路复用中，不同的子信道通过帧内时间片位置予以区分，基于子信道的信息传输周期性地占用帧中的固定时间片，只要收发双方在时间上严格保持同步，双方就可以从复用的信道中分解出所需的信息。同步传输模式最大的特点是时间片的静态分配，而空闲时间片浪费了信道的带宽。

当同步传输模式技术引入交换机时，出现了同步时分交换技术，将输入端口的某个时间片的内容“交换”到输出端对应的时间片中。

2. 异步传输模式

异步传输模式(ATM)：以异步时分复用概念为基础，每个时间片没有固定的占有者，各子信道的信息按照优先级和排队规则按需分配时间片。为了使得接收方可以区分使用时间片的信息所属，信息的前部增加了报头。报头和信息构成了信道上传输的分组。异步传输模式中的分组定义为 53 字节，也称为信元。ATM 是以信元为传输单位的统计复用技术。

当异步传输模式技术引入交换机时，出现了 ATM 交换技术，根据输入端口的各个信元的信元头中的信息将信元“交换”到指定的输出端口。

2.2.4.3　ATM 网络

采用 ATM 交换技术构造的网络称为 ATM 网络。ATM 网络主要包含物理层和数据链路层。其中，数据链路层又被划分为两个子层：ATM 适配子层(AAL)和 ATM 子层。AAL 子层主要定义高层 PDU 和信元中数据域(48 字节)的装拆方法。ATM 子层主要定义信元头的结构，以及 ATM 信元的组织结构等。ATM 物理层主要定义物理设备和物理媒体的接口，以及信元的传输编码等。

1. ATM 物理层

ATM 物理层又分为两个子层：物理介质相关子层(PMD)和传输汇聚子层(TC)。PMD 子层负责在物理媒体上正确传输和接收比特流。TC 子层实现信元流和比特流的转换。

2. ATM 层

ATM 层是 ATM 数据链路层的下子层，主要定义信元头的结构，以及使用物理链路的方法。

1) 信元头结构

ATM 层定义了两种信元头结构：网络用户端接口(UNI)定义了 ATM 交换机面向用户的信元头格式；网络/网络端接口(NNI)定义了 ATM 交换机之间的接口信元头格式。在两种信元头格式中，VPI 用来标识不同的虚拟路径；VCI 用来标识虚拟路径中的虚拟通道。VPI/VCI 在用户建立连接时分配，并在信息传输途径的 ATM 交换节点上建立输入/输出映射表。传输信元时，交换机根据信元头的 VPI/VCI 查映射表，形成新的 VPI/VCI，填入信元头，物理层的 TC 子层形成新的循环冗余校验码，并通过媒体进行传输。

2) ATM 层的功能

ATM 层提供下列功能。

- 信元的汇集和分拣。
- VPI/VCI 的管理。
- 信元头的增删。
- 信元速率调整。

3. ATM 适配层

ATM 适配层(AAL)的主要目的是将高层的信息转换成适合 ATM 网络传输要求的格式。

1) CCITT 通信业务分类

- CLASS A：支持源/宿之间具有实时性要求的恒定位速率(CBR)业务。CBR 业务采用面向连接的工作方式。
- CLASS B：支持源/宿之间具有实时性要求的可变位速率(VBR)业务。VBR 业务采用面向连接的工作方式。
- CLASS C：支持源/宿之间无实时性要求的可变位速率(VBR)业务。
- CLASS D：支持面向无连接的数据传输服务。

其中，CLASS A/B 支持实时信息的传输(如视频和语音传输)，CLASS C/D 支持无实时性要求的信息传输(如高速数据传输)。

2) AAL 协议类型

为了支持上述 4 种类别的业务，CCITT 定义了 4 种类型的 AAL 协议，如表 2.3 所示。

表 2.3 AAL 分类

服务类型	协 议			
	AAL1	AAL2	AAL3/4	AAL5
连接模式	面向连接	面向连接	面向无连接	面向连接
端到端定时	要求	要求	不要求	不要求
位速率	恒定	可变	可变	可变
业务类型	CLASS A	CLASS B	CLASS C/D	CLASS C/D

2.3 真题详解

试题 1 (2017 年下半年试题 18)

下列分组交换网络中，采用的交换技术与其他 3 个不同的是__(18)__网。

(18) A. IP　　B. X. 25　　C. 帧中继　　D. ATM



参考答案：(18)A。

要点解析：IP 是面向对象的连接，其他是面向连接的网络。

试题 2　(2017 年上半年试题 17 和试题 18)

路由器与计算机串行接口连接，利用虚拟终端对路由器进行本地配置的接口是__(17)__，路由器通过光纤连接广域网的接口是__(18)__。

(17) A. Console 口　　B. 同步串行口　　C. SFP 端口　　D. AUX 端口

(18) A. Console 口　　B. 同步串行口　　C. SFP 端口　　D. AUX 端口

参考答案：(17)A；(18)C。

要点解析：路由器 Console 端口使用专用连线直接连接至计算机的串口，对路由器进行本地设置。SFP(Small Form-factor Pluggable，小型机架可插拔设备)端口用于安装 SFP 模块，该模块能够将电、光信号进行转换，可用于连接光纤通道。

试题 3　(2016 年下半年试题 12)

点对点协议 PPP 中 LCP 的作用是__(12)__。

(12) A. 包装各种上层协议　　B. 封装承载的网络层协议

C. 把分组转变成信元　　D. 建立和配置数据链路

参考答案：(12)D。

要点解析：PPP 协议是工作于数据链路层的点到点协议，其包含 LCP 和 NCP 协议，其中 LCP 负责链路的建立、维护和终止；NCP 负责网络层协议的协商。

试题 4　(2016 年下半年试题 50)

由于内网 P2P、视频流媒体、网络游戏等流量占用过大，影响网络性能，可以__(50)__来保障正常的 Web 及邮件流量需求。

(50) A. 使用网闸　　B. 升级核心交换机

C. 部署流量控制设备　　D. 部署网络安全审计设备

参考答案：(50)C。

要点解析：流量控制设备可对不同的业务流量通过带宽保证、带宽预留等流量保障手段，保障关键业务的带宽需求；通过链路备份、流量分担等智能选路策略，保障关键业务的正常使用，极大提升应用的服务质量。

试题 5　(2016 年上半年试题 18)

在 xDSL 技术中，能提供上下行信道非对称传输的技术是__(18)__。

(18) A. HDSL　　B. ADSL　　C. SDSL　　D. ISDNDSL

参考答案：(18)B。

要点解析：数字用户线路(Digital Subscriber Line，DSL)允许用户在传统的电话线上提供高速的数据传输，用户计算机借助于 DSL 调制解调器连接到电话线上，通过 DSL 连接访问因特网络或者企业网络。

DSL 采用尖端的数字调制技术，可以提供比 ISDN 快得多的速率，其实际速率取决于 DSL 的业务类型和很多物理层因素，例如电话线的长度、线径、串扰和噪音等。

DSL 技术存在多种类型，以下是常见的技术类型。

- ADSL：非对称 DSL，上下行流量不对称，一般具有三个信道，分别为 1.544～9Mb/s 的高速下行信道，16～640Kb/s 的双工信道，64Kb/s 的语音信道。
- SDSL：对称 DSL，用户的上下行流量对称，最高可以达到 1.544Mb/s。
- ISDNDSL：介于 ISDN 和 DSL 之间，可以提供最远距离为 4600～5500m 的 128Kb/s 双向对称传输。
- HDSL：高比特率 DSL，是在两个线对上提供 1.544Mb/s 或在三个线对上提供 2.048Mb/s 对称通信的技术，其最大特点是可以运行在低质量线路上，最大距离为 3700～4600m。
- VDSL：甚高比特率 DSL，一种快速非对称 DSL 业务，可以在一对电话线上提供数据和语音业务。

试题 6　(2016 年上半年试题 67)

使用 ADSL 拨号上网，需要在用户端安装__(67)__协议。

(67) A. PPP　　B. SLIP　　C. PPTP　　D. PPPoE

参考答案：(67)D。

要点解析：PPPoE 是利用以太网发送 PPP 并且支持在同一以太网上建立多个 PPP 连接的接入技术，它结合了以太网和 PPP 连接的综合属性，在 ADSL 拨号中经常应用。PPPoE 一般面向广大普通用户提供认证、计费服务，也可用于固定用户申请独用的一个公网 IP 地址。PPPoE 认证的主要特点在于其应用广泛、成熟，而且标准性、互通性好，与现有主流的 PC 操作系统可以良好地兼容，不存在兼容性问题。

试题 7　(2015 年下半年试题 18 和试题 19)

ADSL 采用__(18)__技术把 PSTN 线路划分为话音、上行和下行三个独立的信道，同时提供电话和上网服务。采用 ADSL 联网，计算机需要通过__(19)__和分离器连接到电话入户接线盒。

(18) A. 对分复用　　B. 频分复用　　C. 空分复用　　D. 码分多址

(19) A. ADSL 交换机　　B. Cable Modem　　C. ADSL Modem　　D. 无线路由器

参考答案：(18)B；(19)C。

要点解析：ADSL 技术采用频分复用技术把普通的电话线分成了电话、上行和下行三个相对独立的信道，从而避免了相互之间的干扰。用户可以边打电话边上网，不用担心上网速率和通话质量下降的情况。理论上，ADSL 可在 5km 的范围内，在一对铜缆双绞线上提供最高 1Mb/s 的上行速率和最高 8Mb/s 的下行速率(也就是我们通常说的带宽)，能同时提供话音和数据业务。

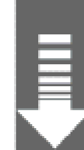
在用户端，用户需要使用一个 ADSL 终端即 ADSL Modem 来连接电话线路。ADSL Modem 的作用是完成数据信号的调制和解调，使数字信号能在模拟信道上传输。

试题 8　(2015 年下半年试题 68 和试题 69)

通过 HFC 网络实现宽带接入，用户端需要的设备是__(68)__，局端用于控制和管理用户的设备是__(69)__。

(68) A. Cable Modem　　B. ADSL Modem

C. OLT　　D. CMTS



(69) A. Cable Modem　　B. ADSL Modem
C. OLT　　D. CMTS

参考答案：(68)A；(69)D。

要点解析：HFC 是将光缆敷设到小区，然后通过光电转换节点，利用有线电视 CATV 的总线式同轴电缆连接到用户，提供综合电信业务的技术。这种方式可以充分利用 CATV 原有的网络，建网快、造价低，逐渐成为最佳的接入方式之一。HFC 是由光纤干线网和同轴电缆分配网通过光节点站结合而成的，一般光纤干线网采用星型拓扑，同轴电缆分配网采用树型结构。

在同轴电缆的技术方案中，用户端需要使用一个称为 Cable Modem(电缆调制解调器)的设备，它不单纯是一个调制解调器，还集成了调谐器、加/解密设备、桥接器、网络接口卡、虚拟专网代理和以太网集线器的功能于一身，无须拨号，可提供随时在线的永久连接。其上行速率已达 10Mb/s 以上，下行速率更高。

CMTS(电缆调制解调器终端系统)，CMTS 是管理控制 Cable Modem 的设备，其配置可通过 Console 接口或以太网接口完成。其配置内容主要有：下行频率、下行调制方式、下行电平等。

试题 9　(2015 年上半年试题 12)

Cisco 路由器高速同步串口默认的封装协议是__(12)__。

(12) A. PPP　　B. LAPB　　C. HDLC　　D. AIM-DXI

参考答案：(12) C。

要点解析：在路由器的广域网连接中，应用最多的端口还要算“高速同步串口”(SERIAL)，这种端口主要是用于连接目前应用非常广泛的 DDN、帧中继(Frame Relay)、X.25、PSTN(模拟电话线路)等网络连接模式，SERIAL 接口支持 HDLC、PPP 和 Frame Relay 的广域网封装协议。HDLC 是 CISCO 路由器使用的缺省协议，一台新路由器在未指定封装协议时默认使用 HDLC 封装。

试题 10　(2015 年上半年试题 33)

以下叙述中，不属于无源光网络优势的是__(33)__。

(33) A. 设备简单，安装维护费用低，投资相对较小
B. 组网灵活，支持多种拓扑结构
C. 安装方便，不用另外租用或建造机房
D. 无源光网络适用于点对点通信

参考答案：(33) D。

要点解析：无光源网络(Passive Optical Network, PON)是一种点对多点的光纤传输和接入技术，下行采用广播方式、上行采用时分多址方式，可以灵活地组成树型、星型、总线型等拓扑结构，在光分支点只需要安装一个简单的光分支器即可，因此具有节省光缆资源、带宽资源共享、节省机房投资、建网速度快、综合建网成本低等优点。无源光网络包括 ATM-PON 和 Ethernet-PON 两种。

2.4 强化训练

2.4.1 综合知识试题

试题 1 (2014 年下半年试题 13)

下面的广域网络中属于电路交换网络的是 (13) 。

(13) A. ADSL　　B. X.25　　C. FRN　　D. ATM

试题 2 (2014 年下半年试题 17 和试题 18)

电信运营商提供的 ISDN 服务有两种不同的接口，其中供小型企业和家庭使用的基本速率接口(BRI)可提供的最大数据速率为 (17) ，供大型企业使用的主速率接口(PRI)可提供的最大数据速率为 (18) 。

(17) A. 128Kb/s　　B. 144Kb/s　　C. 1024Kb/s　　D. 2048Kb/s
(18) A. 128Kb/s　　B. 144Kb/s　　C. 1024Kb/s　　D. 2048Kb/s

试题 3 (2014 年下半年试题 19)

PPP 是连接广域网的一种封装协议，下面关于 PPP 的描述中错误的是 (19) 。

(19) A. 能够控制数据链路的建立　　B. 能够分配和管理广域网的 IP 地址
C. 只能采用 IP 作为网络层协议　　D. 能够有效地进行错误检测

试题 4 (2014 年下半年试题 20 和试题 21)

下面关于帧中继的描述错误的是 (20) ，思科路由器支持的帧中继本地管理接口类型(Lmi-type)不包括 (21) 。

(20) A. 在第三层建立虚电路
B. 提供面向连接的服务
C. 是一种高效率的数据链路技术
D. 充分利用了光纤通信和数字网络技术的优势

(21) A. Cisco　　B. OCE　　C. ANSI　　D. Q933A

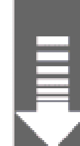
2.4.2 综合知识试题参考答案

【试题 1】答　案：(13) A。

解　析：广域网的通信方式有三种：点到点连接、电路交换和分组交换。现有的电话网络主要是基于电路交换的网络。

ADSL 属于 DSL 技术的一种，全称为 Asymmetric Digital Subscriber Line(非对称数字用户线路)，亦可称作非对称数字用户环路，是一种新的数据传输方式。ADSL 技术采用频分复用技术把普通的电话线分成了电话、上行和下行三个相对独立的信道，从而避免了相互之间的干扰。

X.25 的正式名称是 “工作在公用数据网上以分组方式工作的数据终端设备(DTE)和数据电路端接设备(DCE)之间的接口”，使用的是分组交换，因此它也常常被称为“X.25 分组



交换网”。

FRN 中继技术是分组交换技术的进一步发展，是在数据链路层上用简化的方法传送和交换数据的一种技术。

ATM 是一项数据传输技术，是实现 B-ISDN 业务的核心技术之一。ATM 是以信元为基础的一种分组交换和复用技术，它是一种为了多种业务设计的通用的面向连接的传输模式。它适用于局域网和广域网，具有高速数据传输率，并支持许多种类型如声音、数据、传真、实时视频、CD 质量音频和图像的通信。

【试题 2】答　案：(17) B；(18) D。

解　析：ISDN 分为窄带 ISDN (Narrowband ISDN, N-ISDN)和宽带 ISDN (Broadband ISDN, B-ISDN)。N-ISDN 的目的是以数字系统代替模拟电话系统，把音频、视频和数据业务在一个网络上统一传输。ISDN 系统提供两种用户接口：即基本速率 2B+D 和基群速率 30B+D。所谓 B 信道是 64Kb/s 的话音或数据信道，而 D 信道是 16Kb/s 或 64Kb/s 的信令信道。对于家庭用户，通信公司在用户住所安装一个第一类网络终接设备 NT1。用户可以在连接 NT1 的总线上最多挂接 8 台设备，共享 2B+D 的 144Kb/s 信道。大型商业用户则要通过第二类网络终接设备 NT2 连接 ISDN，这种接入方式可以提供 30B+D (2.048Mb/s)的接口速率。

【试题 3】答　案：(19) C。

解　析：点对点协议(PPP)为在点对点连接上传输多协议数据包提供了一个标准方法。PPP 最初设计是为两个对等节点之间的 IP 流量传输提供一种封装协议。在 TCP/IP 协议集中它是一种用来同步调制连接的数据链路层协议(OSI 模型中的第二层)，替代了原来非标准的第二层协议，即 SLIP。除了 IP 以外，PPP 还可以携带其他协议，包括 DECnet 和 Novell 的 Internet 网包交换(IPX)。

【试题 4】答　案：(20)A；(21) B。

解　析：帧中继在第二层建立虚电路，用帧方式承载数据业务。本地管理接口(LMI)是在 DTE 设备和 FR 之间的一种信令标准，它负责管理链路连接和保持设备间的状态。Cisco 路由器支持的 LMI 标准有 Cisco、ANSI T1.617 ANNEX D、ITU-TQ.933 ANNEX A。

第 3 章 局域网与城域网

3.1 备考指南

3.1.1 考纲要求

根据考试大纲中相应的考核要求，在“局域网与城域网”知识模块上，要求考生掌握以下方面的内容。

(1) IEEE 体系结构。
(2) 以太网。
(3) 网络连接设备。
(4) 高速 LAN 技术。
(5) VLAN。
(6) 无线 LAN。
(7) CSMA/CA。

3.1.2 考点统计

“局域网与城域网”知识模块在历次网络工程师考试试卷中出现的考核知识点及分值分布情况如表 3.1 所示。

表 3.1 历年考点统计表

年 份	题 号	知 识 点	分 值
2017 年下半年	上午：26、62、66、68、70	以太网传输、VLAN、生成树 STP 协议	5 分
	下午：无	无	0 分

续表

年　份	题　号	知 识 点	分　值
2017 年上半年	上午：19	IEEE 802.3 标准	1 分
	下午：无	无	0 分
2016 年下半年	上午：11、60～64	冲突域与广播域、STP 协议、VLAN、网络设备的基本概念	5 分
	下午：无	无	0 分
2016 年上半年	上午：59～63	VLAN、VTP 协议、高速以太网、生成树协议 STP	5 分
	下午：无	无	0 分
2015 年下半年	上午：12、13、66	生成树协议、静态路由命令、虚拟局域网	3 分
	下午：无	无	0 分
2015 年上半年	上午：22、23、33、60	VLAN、生成树协议、无源光网络、MAC 地址	4 分
	下午：无	无	0 分
2014 年下半年	上午：26、27、63、65	城域以太网、VLAN	4 分
	下午：无	无	0 分
2014 年上半年	上午：23～27、50	VLAN、城域以太网	6 分
	下午：无	无	0 分
2013 年下半年	上午：23、26、27、66、67	VTP 协议、无线局域网标准、无线局域网使用的频段	10 分
	下午：无	无	0 分
2013 年上半年	上午：19、61～63、65、66	VTP 协议、生成树协议 STP、VLAN、IEEE 802.1q 协议、光纤以太网传输、CSMA/CA 协议	12 分
	下午：无	无	0 分
2012 年下半年	上午：62～64	CSMA/CD 协议、以太网帧结构、CSMA/CA 协议	6 分
	下午：无	无	0 分
2012 年上半年	上午：63、64	局域网标准、CSMA/CA 协议	4 分
	下午：无	无	0 分

3.1.3　命题特点

纵观历年试卷，本章知识点是以选择题的形式出现在试卷中的。本章知识点在历次考试上午试卷中，所考查的题量大约为 7 道选择题，所占分值为 7 分(约占试卷总分值 75 分中的 9%)；在下午试卷中没有相关考题。本章考题主要检验考生是否理解相关的理论知识点，考试难度较低。在最近两次考试中，题量有所增加，要重点掌握以太网、无线局域网标准和虚拟局域网这三大部分。

3.2　考点串讲

3.2.1　局域网技术基础

3.2.1.1　拓扑结构和传输介质

1. 总线拓扑

总线是一种多点介质，所有的站点都通过接口硬件连接到总线上。工作站发出的数据

组成帧，数据帧沿着总线向两端传播，到达末端的信号被终端匹配器吸收。由于总线是共享介质，多个站同时发送数据时会产生冲突，因而需要一种解决冲突的介质访问协议。传统的轮询方式不适合分布式控制，通常采用分布式竞争发送的访问控制方式。

适用于总线拓扑的传输介质有双绞线、同轴电缆和光纤。双绞线价格便宜，便于安装；而同轴电缆和光纤则能提供更高的数据速率，连接更多的设备，传输的距离也更远。

2. 环型拓扑

环型拓扑由一系列首尾相接的中继器组成，每个中继器连接一个工作站。中继器是一种简单的设备，它能从一端接收数据，然后从另一端发出数据。整个环路是单向传输的。

由于环网是一系列点对点链路串接起来的，所以可使用任何传输介质。最常用的传输介质是双绞线，因为它的价格较低；使用同轴电缆可得到较高的带宽，而光纤则能提供更高的数据速率。

3. 星型拓扑

星型拓扑中有一个中心节点，所有的站点都连接到中心节点上。中心节点在星型网络中起到控制和交换的作用，是网络中的关键设备。

用星型拓扑结构也可以构成分组广播式的局域网。在这种网络中，每个站点都用两对专线连接到中心节点上，一对用于发送，一对用于接收。中心节点叫作集线器，简称 Hub。Hub 接收工作站发来的数据帧，然后向所有的输出链路广播出去。当有多个站点同时向 Hub 发送数据时就会产生冲突，这种情况和总线拓扑中的竞争发送一样，因而总线网的介质访问控制方法也适用于星型网。

3.2.1.2 IEEE 802 标准

IEEE 802 委员会成立于 1980 年 2 月，它的任务是制定局域网的国际标准，目前有 20 多个分委员会。它们制定的部分标准如图 3.1 所示。

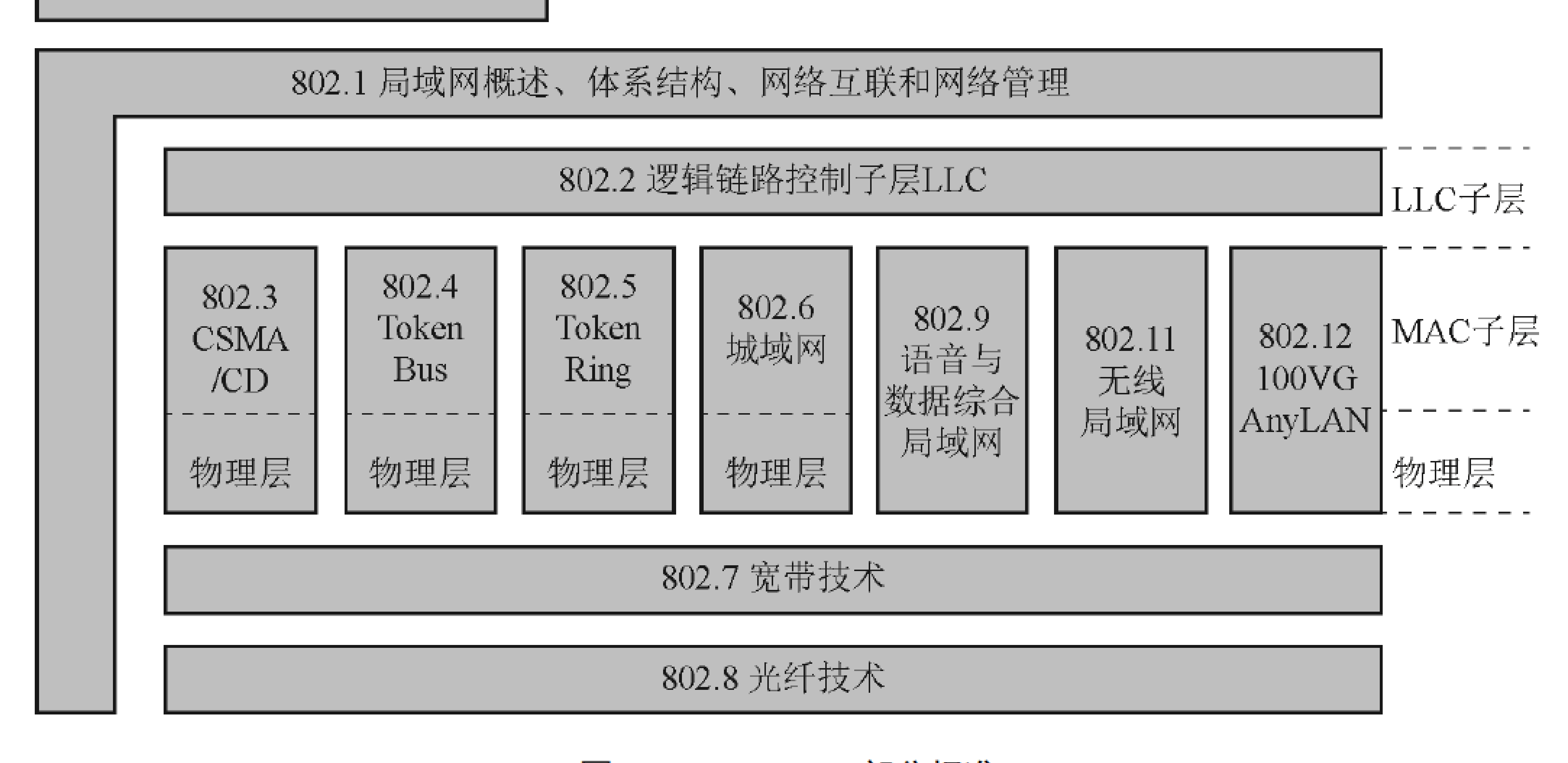


图 3.1　IEEE 802 部分标准

此外还有 803.14、803.15、803.16、803.17、803.18、803.19、803.20 工作组。

- 803.14：采用线缆调制解调器的交互式电视介质访问控制协议及物理层技术规范。
- 803.15：采用蓝牙技术的无线个人网技术规范。
- 803.16：宽带无线接入工作组，开发 2 G～66 GHz 的无线接入系统空中接口。
- 803.17：弹性分组环工作组，制定了弹性分组环网访问控制协议及其有关标准。
- 803.18：宽带无线局域网技术咨询组。
- 803.19：多重虚拟局域网共存技术咨询组。
- 803.20：移动宽带无线接入工作组，正在制定宽带无线接入网的解决方案。

由于局域网使用多种传输介质，而介质访问协议又与具体的传输介质和拓扑结构有关，所以 IEEE 802 标准把数据链路层划分成两个子层，即 MAC 子层和 LLC 子层，如图 3.2 所示，把与访问各种传输介质有关的问题都放入 MAC 子层，而把数据链路层中与介质访问无关的部分都放入 LLC 子层。

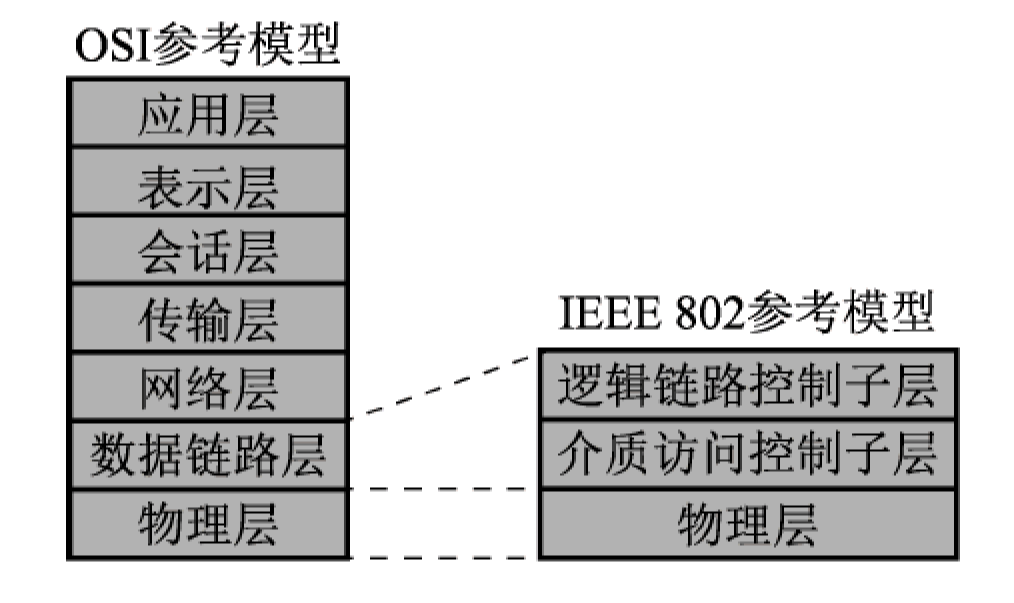


图 3.2　局域网参考模型与 OSI 参考模型的关系

3.2.1.3　逻辑链路控制子层

逻辑链路控制子层(LLC)是 ISO OSI/RM 数据链路层(DL)的高子层，其目的是屏蔽不同的介质访问控制方法，以向高层(网络层)提供统一的服务和接口。从总体上来看，LLC 子层的数据传输和处理流程包括接收来自高层实体(网络层实体)的信息，加上 LLC 子层的控制信息，组合成 LLC 帧，并通过 LLC/MAC 的接口，将 LLC 帧填入 MAC 帧中的 DATA 字段，由 MAC 实体负责传递到接收方。接收方的 LLC 实体调用 MAC 层的服务原语，获得对等实体发来的 LLC 帧。LLC 帧的格式如图 3.3 所示。

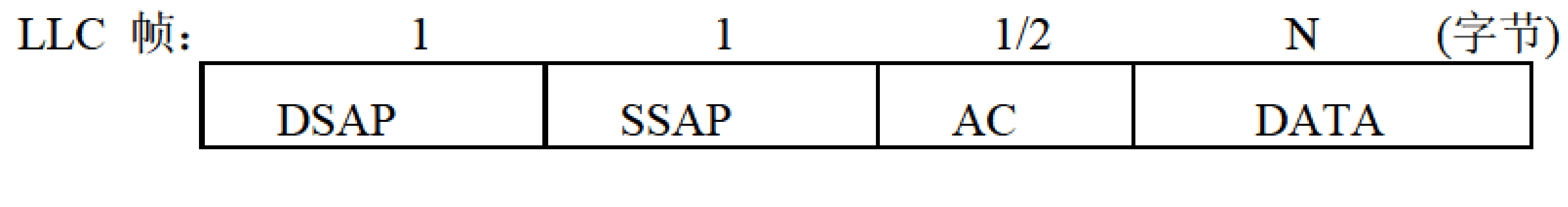


图 3.3　LLC 帧格式

目标/源地址(DSAP/SSAP)各占一个字节，LLC 地址是一个逻辑地址，用于标识一个高层实体可以访问的端口。DSAP 中的第 1 位为单/组地址标识(I/G)，表示本帧发往某个节点(由 MAC 帧中的目的地址指定)上的一个或一组端口；后 7 位表示端口号。SSAP 中的第 1 位为命令/响应标识(C/R)，表示本帧为命令或者响应帧。

1. LLC 地址

LLC 地址是 LLC 层的服务访问点。IEEE 802 局域网中的地址分两级表示，主机的地址是 MAC 地址。LLC 地址实际上是主机中上层协议实体的地址。一个主机中可以同时有多

个上层协议进程，因而就有多个服务访问点。IEEE 802.2 中的地址字段分别用 DSAP 和 SSAP 表示目标地址和源地址，这两个地址都是 7 位长。另外增加的一种功能是可提供组目标地址，而全 1 的地址表示所有用户。在源地址字段中的控制位 C/R 用于区分命令帧和响应帧。

2. LLC 服务

LLC 提供如下 3 种服务。

- 无确认无连接的服务。这是数据报类型的服务。这种服务因其简单而且不涉及任何流控和差错控制功能，因而也不保证可靠地提交。使用这种服务的设备必须在高层软件中处理可靠性的问题。
- 连接方式的服务。这种服务类似于 HDLC 提供的服务。它在有数据交换的用户之间建立连接，同时也通过连接提供流控和差错控制功能。
- 有确认无连接的服务。这种服务与前面两种服务有所交叉，它提供有确认的数据包，但不建立连接。

3. LLC 协议

LLC 协议与 HDLC 协议兼容，它们之间的区别如下。

- LLC 用无编号信息帧支持无连接的服务，这叫作 LLC1 型操作。
- LLC 用 HDLC 的异步平衡方式的操作支持连接方式的 LLC 服务，这种操作叫作 LLC2 型操作。LLC 不支持 HDLC 的其他操作。
- LLC 用两种新的无编号帧支持有确认无连接的服务，这叫作 LLC3 型操作。
- 通过 LLC 服务访问点支持多路复用，即一对 LLC 实体间可建立多个连接。

3.2.1.4 介质访问控制(MAC)技术

在局域网和城域网中，所有设备共享传输介质，所以需要一种方法能有效地分配传输介质的使用权，这种功能就叫作介质访问控制协议。根据控制器位置的不同，介质访问控制协议可分为集中式和分布式。根据控制方式的不同，介质访问控制协议可分为同步式和异步式，而异步分配方法又可分为循环、预约和竞争 3 种方式。

3.2.2 IEEE 802.3 标准

3.2.2.1 CSMA/CD 协议

CSMA/CD 是一种适用于总线结构的分布式介质访问控制方法，是 IEEE 802.3 的核心协议。CSMA 的基本原理是站在发送数据之前，先监听信道上是否有别的站发送的载波信号(若有，说明信道正忙；否则信道是空闲的)，然后根据预定的策略决定。

- 若信道空闲，是否立即发送。
- 若信道忙，是否继续监听。

1. 监听算法

监听算法并不能完全避免发送冲突，但若对以上两种控制策略进行精心设计，则可以把冲突概率减到最小。据此，有以下 3 种监听算法。



1) 非坚持型监听算法

当一个站准备好帧，发送之前先监听信道。

(1) 若信道空闲，立即发送；否则转(2)。

(2) 若信道忙，则后退一个随机时间，重复(1)。

由于随机时延后退，从而减少了冲突的概率；然而，可能出现的问题是因为后退而使信道闲置一段时间，这使信道的利用率降低，而且增加了发送时延。

2) 1-坚持型监听算法

当一个站准备好帧时，发送之前先监听信道。

(1) 若信道空闲，立即发送；否则转(2)。

(2) 若信道忙，继续监听，直到信道空闲后再发送。

这种算法的优缺点与前一种正好相反：有利于抢占信道，减少信道空闲时间；但是多个站同时都在监听信道时必然发生冲突。

3) P-坚持型监听算法

这种算法吸取了以上两种算法的优点，但较为复杂。

(1) 若信道空闲，以概率 P 发送，以概率$(1-P)$延迟一个时间单位。一个时间单位等于网络传输时延 τ 。

(2) 若信道忙，继续监听直到信道空闲，转(1)。

(3) 若发送延迟一个时间单位 τ ，则重复(1)。

2. 冲突检测(CD)原理

载波监听只能减小冲突的概率，而不能完全避免冲突。当两个帧发生冲突后，若继续发送，将会浪费网络带宽。如果帧比较长，对带宽的浪费就很可观。为了进一步改进带宽的利用率，发送站应采取边发边听的冲突检测方法，具体如下。

(1) 发送期间同时接收，并把接收的数据与站中存储的数据进行比较。

(2) 若比较结果一致，说明没有冲突，重复(1)。

(3) 若比较结果不一致，说明发生冲突，立即停止发送，并发送一个简短的干扰信号(Jamming)，使所有站都停止发送。

(4) 发送 Jamming 信号后，等待一段随机长的时间，重新监听，再试着发送。

3. 二进制指数后退算法

按照二进制指数后退算法，后退时延的取值范围与重发次数 n 形成二进制指数关系。随着重发次数 n 的增加，后退时延 t_ζ 的取值范围按 2 的指数增大。即第一次试发时 n 的值为 0，每冲突一次 n 的值加 1，并按式(3.1)计算后退时延。

$$\begin{cases} \zeta = \text{random}[0,\ 2^n] \\ t_\zeta = \zeta_\tau \end{cases} \tag{3.1}$$

为了避免无限制的重发，要对重发次数 n 进行限制。通常当 n 增加到某一个最大值时停止发送，并向上层协议报告发送错误，等待处理。

4. CSMA/CD 的实现

对于基带总线和宽带总线，CSMA/CD 的实现基本上是相同的，但也有一些差别。

差别一是载波监听的实现。对于基带系统，是检测电压脉冲序列。对于宽带系统，监

听站接收 RF 载波以判断信道是否空闲。

差别二是冲突检测的实现。对于基带系统，是把直流电压加到信号上来检测冲突。对于宽带系统，有两种检测冲突的方法：一种方法是把接收的数据与发送的数据逐位比较；另一种方法用于分裂配置，由端头检查是否有破坏了的数据，这种数据的频率与正常数据的频率不同。

5. 性能分析

吞吐率是单位时间内实际传送的位数。假设网上的站点都有数据要发送，没有竞争冲突，各站轮流发送数据，则传送一个长度为 L 的帧的周期为 t_p+t_f。由此可得出最大吞吐率为

$$T=\frac{L}{t_p+t_f}=\frac{L}{d/v+L/R} \tag{3.2}$$

其中：d 表示网络段长；v 表示信号在铜线中的传播速度(大约为光速的 65%～77%)；R 为网络提供的数据速率，或称为网络容量。

同时可得出网络利用率为

$$E=\frac{T}{R}=\frac{L/R}{d/v+L/R}=\frac{t_f}{t_p+t_f} \tag{3.3}$$

利用 $a=t_p/t_f$，得

$$E=\frac{1}{a+1} \tag{3.4}$$

其中，a(或者 Rd 的乘积)越大，信道利用率越低。

3.2.2.2 传统以太网

最早采用 CSMA/CD 协议的网络是 Xerox 公司的以太网。1981 年，DEC、Intel 和 Xerox 三家公司制定了 DIX 以太网标准。后来，IEEE 802 委员会参考了以太网标准制定了局域网标准。以太网是 803.3 标准中的一种。

1. MAC 帧结构

CSMA/CD 方式定义的帧结构内含有 8 个字段：前导码(P)、帧起始符(SFD)、目的地址(DA)、源地址(SA)、数据长度(L)、用户数据(DATA)、填充字段(PAD)和帧校验序列(FCS)。完整的 MAC 帧格式如图 3.4 所示。

7	1	2/6	2/6	2	0～1500	0～46	4	(字节)
P	SFD	DA	SA	L	DATA	PAD	FCS	

图 3.4　CDMA/CD 的 MAC 帧格式

- 前导码字段(P)包含 7 个字节，其格式为“1010..1010”。前导码的目的是使接收端进入同步状态，以便数据的接收。
- 帧起始符(SFD)占一个字节，取值为 10101011。SFD 紧跟在前导码字段之后，标识本信息帧的开始。
- 目的地址/源地址(DA/SA)各占 2 个或 6 个字节，10 Mb/s 的基带网络只使用 6 字节地址。目的地址最高位为 0 时表示普通地址，为 1 时表示组地址。全 1 的目的地址是广播地址，所有站都接收这种帧。地址字段的次高位表示采用本地地址或者



全局地址，本地地址为两字节地址，由网络管理员分配；全局地址为 6 字节地址，由 IEEE 分配，确保全球唯一。尽管标准中定义的地址字段可以是 2 个或者 6 个字节，但在同一个网络中地址结构应当一致。

- 数据字段长度(L)占 2 个字节，表示 DATA 字段的实际长度。
- 用户数据字段(DATA)小于 1500 个字节，用于存放高层 LLC 的信息。
- 填充字段(PAD)不大于 46 个字节。为了保证帧发送期间能检测到冲突，IEEE 803.3 规定最小帧为 64 字节。这个帧长是指从目标地址到校验序列的长度。由于前导码和帧起始符是物理层加上的，所以不包括在帧长中，也不参加帧校验。如果帧的长度不足 64 字节，就要加入最多 46 字节的填充位。
- 帧校验序列(FCS)占 4 个字节，采用循环冗余校验码。

2. CSMA/CD 协议的实现

IEEE 803.3 采用 CSMA/CD 协议，这个协议的载波监听、冲突检测、冲突强化、二进制指数后退等功能都由硬件来实现。这些硬逻辑电路包含在网卡中。网卡上的主要器件是以太网数据链路控制器(Ethernet Data Link Controller，EDLC)。这个器件中有两套独立的系统，分别用于发送和接收。

IEEE 803.3 使用 1-坚持型监听算法，因为这个算法可及时抢占信道，减少空闲期，同时实现也较简单。在监听到网络由活动变为安静后，它并不能立即开始发送，还要等待一个最小帧间隔时间，只有在此期间网络持续平静，才能开始试发送。最小帧间隔时间规定为 9.6 μs。

在发送过程中继续监听。若检测到冲突，发送 8 个十六进制数的序列 55555555，这就是协议规定的阻塞信号。

接收站要对收到的帧进行校验。除了 CRC 校验之外，还要检查帧的长度。短于最小长度的帧被认为是冲突碎片而丢弃，帧长与数据长度不一致的帧以及长度不是整数字节的帧也被丢弃。

3. 物理层规范

表 3.2 所示的是 IEEE 803.3 所采用的传输介质。

表 3.2　IEEE 803.3 的传输介质

项　目	以 太 网	10Base-5	10Base-2	1Base-5	10Base-T	10Broad-36	10Base-F
拓扑结构	总线型	总线型	总线型	星型	星型	总线型	星型
数据速率/(Mb/s)	10	10	10	1	10	10	10
信号类型	基带曼码	基带曼码	基带曼码	基带曼码	基带曼码	宽带 DPSK	基带曼码
最大段长/m	500	500	200	250	100	360	500，2000
传输介质	粗同轴电缆	粗同轴电缆	细同轴电缆	UTP	UTP	CATV 电缆	光纤

3.2.2.3　高速以太网

1. 快速以太网

1995 年，100 Mb/s 的快速以太网标准 IEEE 803.3u 正式颁布，这是基于 10Base-T 和

10Base-F 技术，在基本布线系统不变的情况下开发的高速局域网标准。

快速以太网使用的集线器可以是共享型或交换型，也可以通过堆叠多个集线器扩大端口数量。互相连接的集线器起到了中继的作用，扩大了网络的跨距。快速以太网使用的中继器分为两类。Ⅰ类中继器中包含了编码/译码功能，它的延迟比Ⅱ类中继器大。

快速以太网中的数据速率提高了 10 倍，而最小帧长没变，所以冲突时槽缩小为 5.12 μs。以太网的计算冲突时槽的公式为

$$\text{solt} \approx 2S/0.7C + 2t_{\text{phy}} \tag{3.5}$$

其中：S 表示网络的跨距(最长传输距离)；$0.7C$ 为 0.7 倍光速(信号传播速率)；t_{phy} 是发送站物理层时延，由于发送站发送和接收两次，所以取其时延的两倍值。

由此可得计算快速以太网跨距的计算公式为

$$S \approx 0.35C(L_{\min}/R - 2t_{\text{phy}}) \tag{3.6}$$

2. 千兆以太网

1000 Mb/s 以太网的传输速率更快，它作为主干网提供无阻塞的数据传输服务。1996 年 3 月 IEEE 成立了 803.3z 工作组，最终制定的 1 Gb/s 的以太网标准包括如下内容。

- 1000Base-CX：使用两对 STP 和 9 芯 D 型连接器，最大段长为 25 m。
- 1000Base-LX：使用一对 63.5 μm 或 50 μm 多模光纤，最大段长为 550 m；或使用 9 μm 的单模光纤，最长距离为 5 km。
- 1000Base-SX：使用一对 63.5 μm 的多模光纤，最大段长为 550 m；或使用一对 50 μm 的多模光纤，最大段长为 525 m。
- 1000Base-TX：使用一对五类 UTP，最大段长为 100 m。

要实现 1000 Mb/s 的数据速率，需要采用许多新的数据处理技术。首先是最小帧长需要扩展，以便在半双工的情况下增加跨距。另外，803.3z 还定义了一种帧突发方式(Frame Bursting)，使得一个站可以连续发送多个帧。最后物理层编码也采用了与 10 Mb/s 不同的编码方式，即 4B/5B 或 8B/9B 编码法。

3. 万兆以太网(10GE)

2002 年 6 月，IEEE 803.3ae 标准发布，支持 10 Gb/s 的传输速率。万兆以太网具有以下特点。

- MAC 子层和物理层实现 10 Gb/s 传输速率。
- MAC 子层的帧格式不变，并保留 IEEE 803.3 标准最小和最大帧长度。
- 不支持共享型，只支持全双工，即只可能实现全双工交换型 10 Gb/s 以太网。
- 支持星型局域网拓扑结构，采用点到点连接和结构化布线技术。
- 在物理层上分别定义了局域网和广域网两种系列。
- 不能使用双绞线，只支持多模和单模光纤。

3.2.3 虚拟局域网

3.2.3.1 VLAN 的概念

VLAN(Virtual Local Area Network)的中文名为“虚拟局域网”。VLAN 是一种将局域网

设备从逻辑上划分成一个个网段，从而实现虚拟工作组的新兴数据交换技术。

VLAN 技术的出现，主要是为了解决交换机在进行局域网互连时无法限制广播的问题。这种技术可以把一个 LAN 划分成多个逻辑的 LAN 即 VLAN，每个 VLAN 是一个广播域，VLAN 内的主机间通信就和在一个 LAN 内一样，而 VLAN 间则不能直接互通，这样，广播报文就被限制在一个 VLAN 内。

VLAN 是建立在物理网络基础上的一种逻辑子网，因此建立 VLAN 需要相应的支持 VLAN 技术的网络设备。当网络中的不同 VLAN 间进行相互通信时，需要路由的支持，这时就需要增加路由设备—— 要实现路由功能，既可采用路由器，也可采用三层交换机来完成。

3.2.3.2　VLAN 的划分方法

1. 根据端口划分 VLAN

许多 VLAN 厂商都利用交换机的端口来划分 VLAN 成员。被设定的端口都在同一个广播域中。例如，一个交换机的 1～5 端口被定义为虚拟网 AAA，而同一交换机的 6～8 端口组成虚拟网 BBB。这样做允许各端口之间的通信，并允许共享型网络的升级。但是，这种划分模式将虚拟网限制在了一台交换机上。

第二代端口 VLAN 技术允许跨越多个交换机的多个不同端口划分 VLAN，不同交换机上的若干端口可以组成同一个虚拟网。

以交换机端口来划分网络成员，其配置过程简单明了。因此，从目前来看，这种根据端口来划分 VLAN 的方式仍然是最常用的一种方式。

2. 根据 MAC 地址划分 VLAN

这种划分 VLAN 的方法是根据每个主机的 MAC 地址来划分，即对每个 MAC 地址的主机都配置它属于哪个组。这种划分方法的最大优点就是，当用户的物理位置移动时，即从一个交换机换到其他交换机时，VLAN 不用重新配置。所以，可认为这种根据 MAC 地址的划分方法是基于用户的 VLAN。这种划分方法的缺点是，初始化时所有的用户都必须进行配置，如果有几百个甚至上千个用户的话，配置是非常麻烦的。而且这种划分方法也导致了交换机执行效率的降低，因为在每一个交换机的端口都可能存在很多个 VLAN 组的成员，这样就无法限制广播包了。另外，对于使用笔记本电脑的用户来说，他们的网卡可能经常更换，这样，VLAN 就必须不停地配置。

3. 根据网络层划分 VLAN

这种划分 VLAN 的方法是根据每个主机的网络层地址或协议类型(如果支持多协议)划分的，虽然这种方法是根据网络地址，比如 IP 地址来划分的，但它不是路由，与网络层的路由毫无关系。

这种划分方法的优点是：如果用户的物理位置改变了，不需要重新配置所属的 VLAN，而且可以根据协议类型来划分 VLAN，这对网络管理者来说很重要；还有，这种方法不需要附加的帧标签来识别 VLAN，这样可以减少网络的通信量。

这种划分方法的缺点是效率低，因为检查每一个数据包的网络层地址是需要消耗处理时间的(相对于前面两种方法)，一般的交换机芯片都可以自动检查网络上数据包的以太网帧

头，但要让芯片能检查 IP 帧头，则需要更高的技术，同时也更费时。当然，这与各个厂商的实现方法有关。

4. 根据 IP 组播划分 VLAN

IP 组播实际上也是一种 VLAN 的定义，即认为一个组播组就是一个 VLAN。这种划分的方法将 VLAN 扩大到了广域网，因此具有更大的灵活性，而且也很容易通过路由器进行扩展。当然，这种方法不适合局域网，主要是因为效率不高。

5. 基于规则的 VLAN

基于规则的 VLAN 也称为基于策略的 VLAN。这是最灵活的 VLAN 划分方法，具有自动配置的能力，能够把相关的用户连成一体，在逻辑划分上称为“关系网络”。网络管理员只需在网管软件中确定划分 VLAN 的规则(或属性)，那么当一个站点加入网络中时，将会被“感知”，并被自动地包含进正确的 VLAN 中。同时，它对站点的移动和改变也可自动识别和跟踪。

采用这种方法，整个网络可以非常方便地通过路由器扩展网络规模。有的产品还支持一个端口上的主机分别属于不同的 VLAN，这在交换机与共享式 Hub 共存的环境中显得尤为重要。自动配置 VLAN 时，交换机中的软件自动检查进入交换机端口的广播信息的 IP 源地址，然后自动将这个端口分配给一个由 IP 子网映射成的 VLAN。

3.2.3.3 VLAN 的标准

对于 VLAN 的标准，我们只介绍两种比较通用的。当然也有一些公司具有自己的标准，比如 Cisco 公司的 ISL 标准，虽然不是一种大众化的标准，但是由于 Cisco Catalyst 交换机的大量使用，ISL 也成为一种不是标准的标准了。

1. 803.10 VLAN 标准

1995 年，Cisco 公司提倡使用 IEEE 803.10 协议。在此之前，IEEE 803.10 曾经在全球范围内作为 VLAN 安全性的同一规范。Cisco 公司试图采用优化后的 803.10 帧格式在网络上传输 Frame Tagging 模式中所必需的 VLAN 标记。然而，大多数 802 委员会的成员都反对推广 803.10，因为该协议是基于 Frame Tagging 方式的。

2. 803.1q

1996 年 3 月，IEEE 803.1 Internet Working 委员会结束了对 VLAN 初期标准的修订工作。新出台的标准进一步完善了 VLAN 的体系结构，统一了 Frame Tagging 方式中不同厂商的标记格式，并制定了 VLAN 标准在未来一段时间内的发展方向，形成的 803.1q 的标准在业界获得了广泛的推广。它成为 VLAN 史上的一块里程碑。803.1q 的出现打破了虚拟网依赖于单一厂商的僵局，从一个侧面推动了 VLAN 的迅速发展。另外，来自市场的压力使各大网络厂商立刻将新标准融合到它们各自的产品中。

3. Cisco ISL 标记

ISL(Inter-Switch Link)是 Cisco 公司的专有封装方式，因此只能在 Cisco 的设备上支持。ISL 是一个在交换机之间、交换机与路由器之间及交换机与服务器之间传递多个 VLAN 信息及 VLAN 数据流的协议，通过在交换机直接的端口配置 ISL 封装，即可跨越交换机进行



整个网络的 VLAN 分配和配置。

3.2.3.4　VLAN 帧标记

IEEE 803.1q 协议定义了 VLAN 帧标记的格式，它在原来的以太帧中增加了 4 个字节的帧标记字段，如图 3.5 所示。其中标记控制信息(Tag Control Information，TCI)包括 Priority、CFI 和 VID 三个部分。

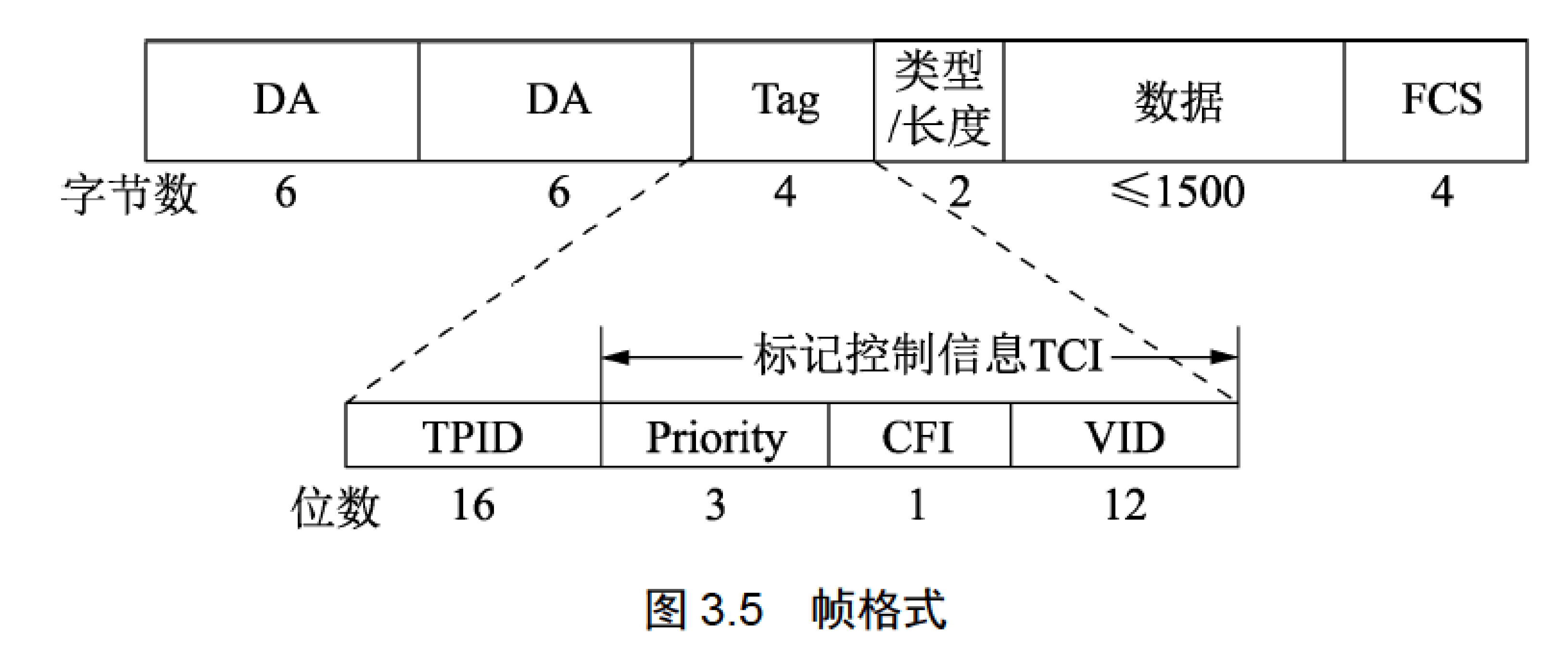


图 3.5　帧格式

- 标记协议标识符字段(Tag Protocol Identifier，TPID)设定为 0x8100，表示该帧包含 803.1q 标记。
- Priority 字段提供了由 803.1q 定义的 8 个优先级。当有多个帧等待发送时，按优先级发送数据包。
- CFI 为规范格式指示(Canonical Format Indicator)，0 表示以太网，1 表示 FDDI 和令牌环网。
- VID 字段表示 VLAN 标识符(0～4095)，其中 VID 0 用于识别优先级，VID 4095 保留未用，所以最多可配置 4094 个 VLAN。

3.2.3.5　虚拟局域网中继

在划分成 VLAN 的交换网络中，交换机端口之间的连接分为两种：接入链路连接(Access-Link Connection)和中继连接(Trunk Connection)。

接入链路只能连接具有标准以太网卡的设备，也只能传送属于单个 VLAN 的数据包。任何连接到接入链路的设备均属于同一广播域。

中继链路是在一条物理连接上生成多个逻辑连接，每个逻辑连接属于一个 VLAN。在进入中继端口时，交换机在数据包中加入 VLAN 标记。这样，在中继链路另一端的交换机就不仅要根据目标地址，而且要根据数据包属于的 VLAN 进行转发决策。

3.2.3.6　VTP 协议与 VTP 修剪

VLAN 中继协议(VTP)用于在交换网络中简化 VLAN 的管理。VTP 协议在交换网络中建立了多个管理域，同一管理域中的所有交换机共享 VLAN 信息。一台交换机只能参加一个管理域，不同管理域中的交换机不共享 VLAN 信息。通过 VTP 协议，可以在一台交换机上配置所有的 VLAN，配置信息通过 VTP 报文可以传播到管理域中的所有交换机上。

VTP 有 3 种工作模式：服务器模式、客户模式和透明模式。其中：服务器模式可以设置 VLAN 信息，服务器会自动将这些信息广播到网上的其他交换机上以统一配置；客户模式下交换机不能配置 VLAN 信息，只能被动接受服务器的 VLAN 配置；透明模式下可以配

置 VLAN 信息，但是不广播自己的 VLAN 信息，同时它可以接收服务器发来的 VLAN 信息后并不使用，而是直接转发给别的交换机。

在默认情况下，所有交换机都通过中继链路连接在一起，如果 VLAN 中的任何设备发出一个广播包、组播包或者一个未知的单播数据包，交换机都会将其洪泛(Flood)到所有与源 VLAN 端口相关的各个输出端口上(包括中继端口)。在很多情况下，这种洪泛转发是必要的，特别是在 VLAN 跨越多个交换机的情况下。然而，如果相邻的交换机上不存在源 VLAN 的活动窗口，则这种洪泛发送的数据包是无用的。

为了解决这个问题，可以使用静态或动态的修剪方法。所谓静态修剪，就是手工剪掉中继链路上不活动的 VLAN。但是，手工修剪会遇到一些问题，主要是必须根据网络拓扑结构的改变经常重新配置中继链路。在多个交换机组成多个 VLAN 的网络中，这种工作方式很容易出错。

VTP 动态修剪允许交换机之间共享 VLAN 信息，也允许交换机从中继连接上动态地剪掉不活动的 VLAN，从而使得所有共享的 VLAN 都是活动的。例如，交换机 A 告诉交换机 B，它有两个活动的 VLAN1 和 VLAN2，而交换机 B 告诉交换机 A，它只有一个活动的 VLAN1，于是，它们就共享这样的事实：VLAN2 在它们之间的中继链路上是不活动的，应该从中继链路的配置中剪掉。这样做的好处显而易见，如果以后在交换机 B 上添加了 VLAN2 的成员，交换机 B 就会通知交换机 A，它有了一个新的活动的 VLAN2，于是，两个交换机就会动态地把 VLAN2 添加到它们之间的中继链路配置中。

3.2.4 局域网互连

局域网用网桥互连，IEEE 802 标准中包含两种关于网桥的规范：透明网桥和源路由网桥。

3.2.4.1 网桥协议的体系结构

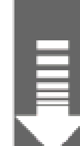
在 IEEE 802 体系结构中，站地址是由 MAC 子层协议来说明的，网桥在 MAC 子层中起中继作用。网桥可以直接连接两个局域网，此时这两个局域网运行相同的 MAC 和 LLC(逻辑链路控制)协议。如果两个局域网相距较远，也可以用两个网桥分别连接一个局域网，两个网桥之间再用通信线路相连(可以是其他网络)。

一个网桥可以连接多个局域网，但网桥连接的局域网多于两个时，网桥必须具有路由选择的功能。为了对网桥的路由选择提供支持，MAC 层地址应当分为两部分：网络地址部分(标识互联网中唯一的局域网)和站地址部分(标识某个局域网中唯一的工作站)。IEEE 803.5 标准建议：16 位 MAC 地址分成 7 位的局域网地址和 8 位的工作站地址，48 位的 MAC 地址分成 14 位的局域网地址和 32 位的工作站地址，其余的位用于区分组地址/单地址，以及局部地址/全局地址。

3.2.4.2 生成树网桥

生成树网桥是一种透明网桥，这个网桥插入电缆后就可自动完成路由选择的功能，无须用户装入路由表或设置参数，桥内部可动态地维护地址映射表。根据该地址映射表，网桥决定收到的帧被转发到对应的子网，或者通过该子网作进一步的转发。

这种网桥的原理很简单：当网桥收到每一个帧时，都执行地址表扩充和帧转发两项工



作。地址表扩充是从帧中取出信源节点地址，并填写地址表，从而使网桥“了解”哪些节点属于哪个子网。帧的转发是网桥根据帧中的信宿节点地址查找地址表，如果表中有对应的地址，帧被转发到指定的网络；否则，转发给本网桥连接的所有子网(广播)。

此类网桥得以实现的关键是假定任意两个局域网之间只有一条唯一的通路。当增加冗余的网桥时，如不采取别的措施，会出现环路问题。解决这个问题的措施是构造基于网桥的支撑树(生成树)。构造支撑树的目的是在增加冗余设备提高网络可靠性的同时，解决网络循环连接带来的问题。

构造支撑树的基本思想是，首先选择网络中的某个网桥(一般选择位置处于相对中心的网桥)作为树的根，然后从与该树(最初只有根)相邻(可以通过某个子网直接访问)的网桥集合中选择一个加入支撑树，选择的条件是加入该网桥不会形成环路。这种选择的过程继续进行，直至支撑树可以互连所有的子网，剩下的网桥留作备用。

3.2.4.3　源路由网桥

源路由网桥的核心思想是，由帧的发送者显式地指明路由信息(RI)。RI 由网桥地址和局域网标识符的序列组成，包含在帧头中。每个收到帧的网桥根据帧头中的地址信息可以知道自己是否在转发路径中，并可以确定转发的方向。

确定路径的基本思想是，如果源节点不知道路径，则发送一个具有测试功能的广播帧，广播帧被每个网桥接收。接到广播帧的网桥检查广播帧中的 RI 字段，如果本网桥号已经在 RI 中，则不作任何处理；否则，向 RI 中增加段号，并将该帧转发到与之连接且网号未在帧中出现的其他子网。当信宿节点接到该测试帧后，向源发节点返回一个应答帧。应答帧中包含了所需的路径信息，并沿着测试帧途经的路径反向传递。由于广播的缘故，源发节点会收到多个应答帧，通过某种算法从中选择一条路径。

源路由网桥可以获得最佳路径，其缺点是测试帧可能会形成“广播风暴”。

3.2.5　城域网

3.2.5.1　城域以太网

1. 城域以太网论坛

城域以太网论坛(MEF)是由网络设备制造商和网络设备运营商组成的非营利性组织，专门从事城域以太网的标准化工作。MEF 的承载以太网(Carrier Ethernet)技术规范提出了以下几种业务类型。

(1) 以太网专用线(EPL)。

(2) 以太网虚拟专线(EVPL)。在一对用户以太网之间通过第三层技术提供点对点的虚拟以太网连接。

(3) 以太局域网服务(E-LAN Services)。

2. E-LAN 服务

提供 E-LAN 服务的基本技术是 803.1q 的 VLAN 帧标记。这种技术定义在 IEEE 803.1ad 的运营商网桥协议(Provider Bridge Protocol)中，被称为 Q-in-Q 技术。

3. 803.1ah 标准

Q-in-Q 实际上是把用户 VLAN 嵌套在城域以太网的 VLAN 中传送，所有用户的 MAC 地址在城域以太网中都是可见的，这使得网络安全受到威胁。因此 IEEE 803.1ah 标准提出了运营商主干网桥(PBB)协议。

3.2.5.2 弹性分组网

弹性分组网(Resilient Packet Ring，RPR)是一种采用环型拓扑的城域网技术。2004 年公布的 IEEE 803.17 标准定义了 RPR 的介质访问控制方法、物理层接口以及层管理参数，并提出了用于环路检测和配置、失效回复以及带宽管理的一系列协议。RPR 支持的数据速率可以达到 10 Gb/s。

1. 体系结构

RPR 的体系结构如图 3.6 所示。RPR 采用了双环结构，由内层的环 1 和外层的环 0 组成，每个环都是单方向传送。相邻工作站之间的跨距包含传送方向相反的两条链路。RPR 支持多达 255 个工作站，最大环周长为 2000 km。

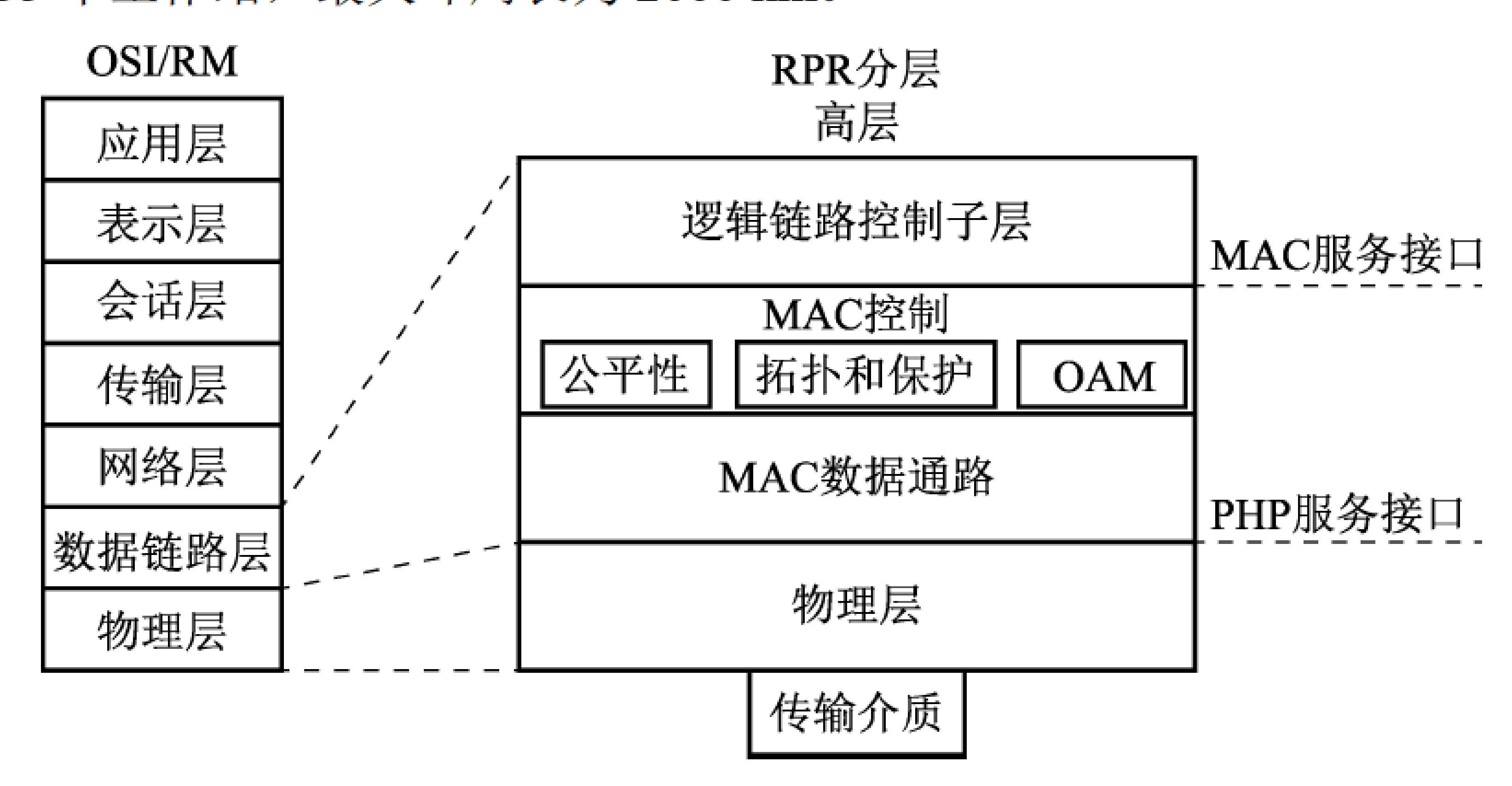


图 3.6 RPR 体系结构

2. RPR 的关键技术

RPR 的关键技术有：业务类型、空间复用、拓扑发现、公平算法、环自愈保护。

3.3 真题详解

试题 1 (2017 年下半年试题 26)

以下关于 VLAN 标记的说法中，错误的是 (26) 。

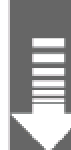
(26) A. 交换机根据目标地址和 VLAN 标记进行转发决策

B. 进入目的网段时，交换机删除 VLAN 标记，恢复原来的帧结构

C. 添加和删除 VLAN 标记的过程处理速度较慢，会引入太大的延迟

D. VLAN 标记对用户是透明的

参考答案：(26) C。



要点解析：VLAN 标记只增加了 4 个字节，在以太帧之外由硬件芯片完成，速度快，不会引起太大的延迟。

试题 2　(2017 年下半年试题 62)

以下关于 VLAN 的叙述中，错误的是__(62)__。

(62) A. VLAN 把交换机划分成多个逻辑上独立的区域
B. VLAN 可以跨越交换机
C. VLAN 只能按交换机端口进行划分
D. VLAN 隔离了广播，可以缩小广播风暴的范围

参考答案：(62) C。

要点解析：VLAN 可以根据交换机端口、MAC 地址、网络层以及 IP 组播来划分。

试题 3　(2017 年下半年试题 68)

下面消除交换机上 MAC 地址漂移告警的方法中，描述正确的是__(68)__。

① 人工把发生漂移的接口 shutdown
② 在接口上配置 error-down，自动 down 掉漂移的端口
③ 在接口上配置 quit-vlan，使发生漂移的接口从指定 VLAN 域内退出
④ 在接口上配置 stp tc-protection 解决 MAC 地址漂移

(68) A. ①②③④　　B. ②③④　　C. ②③　　D. ①②③

参考答案：(68) D。

要点解析：MAC 地址漂移是指在同一个 VLAN 内，一个 MAC 地址有两个出接口，并且后学习到的出接口覆盖原出接口的现象，也就是指 MAC 地址表项的出接口发生了变更。消除 MAC 地址漂移的方法有三种：①人工把漂移的接口 shutdown；②通过在接口上配置漂移检测动作 error-down，自动 down 掉漂移的端口；③通过在接口上配置漂移检测动作 quit-vlan，使漂移的接口从指定的 VLAN 域内退出，从而消除 MAC 地址漂移，破坏环路。

试题 4　(2017 年下半年试题 70)

某 STP 网络从链路故障中恢复时，端口收敛时间超过 30 秒，处理该故障的思路不包括__(70)__。

(70) A. 确认对端端口开启 STP
B. 确认端口是工作在 STP 模式
C. 确认端口的链路类型是点对点
D. 确认端口模式为中继模式

参考答案：(70) D。

要点解析：STP 的网络拓扑中出现链路故障或链路故障恢复后，业务流量恢复需要超过 30 秒，即端口无法快速收敛，此时需要：①确认对端端口是否使能 STP；②检查端口是否工作在 STP 模式；③检查端口的链路类型是否为点对点。

试题 5　(2017 年上半年试题 19)

1996 年 3 月，IEEE 成立了 802.3z 工作组开始制定 1000Mb/s 标准。下列千兆以太网中不属于该标准的是__(19)__。

(19) A. 1000Base-SX　B. 1000Base-LX　C. 1000Base-T　D. 1000Base-CX

参考答案：(19) C。

要点解析：千兆以太网标准包括 1000Base-CX、1000Base-LX、1000Base-SX、1000Base-TX 四种。

试题 6 (2016 年下半年试题 11)

能隔离局域网中广播风暴、提高带宽利用率的设备是 (11) 。

(11) A. 网桥　B. 集线器　C. 路由器　D. 交换机

参考答案：(11) C。

要点解析：路由器不转发广播包，可以避免广播风暴。

试题 7 (2016 年下半年试题 60)

STP 协议的作用是 (60) 。

(60) A. 防止二层环路　B. 以太网流量控制
C. 划分逻辑网络　D. 基于端口的认证

参考答案：(60)A。

要点解析：STP 协议的作用是防止二层环路，通过阻塞部分端口，将网络修剪成树型结构。一般来说，产生交换环路会造成广播风暴，使交换机处于忙碌状态，阻塞正常的网络流量，还会造成 MAC 地址表不稳定，而利用 STP 协议正好可以解决这个问题。

试题 8 (2016 年下半年试题 61)

VLAN 之间通信需要 (61) 的支持。

(61) A. 网桥　B. 路由器　C. VLAN 服务器　D. 交换机

参考答案：(61) B。

要点解析：网络中不同的 VLAN 间进行相互通信的时候，需要路由器的支持，实现路由功能，既可采用路由器，也可采用三层交换机来完成。D 选项交换机默认为二层交换机。

试题 9 (2016 年下半年试题 62)

以太网中出现冲突后，发送方什么时候可以再次尝试发送？ (62)

(62) A. 再次收到目标站的发送请求后
B. 在 JAM 信号停止并等待一段固定时间后
C. 在 JAM 信号停止并等待一段随机时间后
D. 当 JAM 信号指标冲突已经被清除后

参考答案：(62) C。

要点解析：CSMA/CD 协议中出现冲突后发送冲突加强信号(JAM 信号)，然后运行后退算法，重新检测，一般使用截断二进制指数退避算法，具体流程如下。

(1) 监测到冲突后，马上停止发送数据，并等待一段时间。

(2) 定义参数 k，k 为重传次数，且 k 不超过 10，k=min[重传次数，10]。

(3) 从整数[0，1，…(2k−1)]中随机取一个数，记为 n，重传退避时间为 n 倍冲突槽时间。

(4) 如果重传次数达到 16 次，就丢弃该帧。



试题 10　(2016 年下半年试题 63 和试题 64)

网桥怎样知道网络端口连接了哪些网站？__(63)__ 当网桥连接的局域网出现环路时怎么办？__(64)__

(63) A. 如果从端口收到一个数据帧，则将其目标地址记入该端口的数据库

B. 如果从端口收到一个数据帧，则将其源地址记入该端口的数据库

C. 向与端口连接的各个站点发送请求以便获取其 MAC 地址

D. 由网络管理员预先配置好各个端口的地址数据库

(64) A. 运行生成树协议阻塞一部分端口

B. 运行动态主机配置协议重新分配端口地址

C. 通过站点之间的协商产生一部分备用端口

D. 各个网桥通过选举产生多个没有环路的生成树

参考答案：(63) B；(64) A。

要点解析：网桥查看每个端口出现的帧，将其源地址记入该端口的数据库，这样就可以了解各个端口连接了哪些网站。当网桥连接的局域网出现环路时，所有的网桥通过运行生成树协议，阻塞一部分端口，使得不再出现环路。

试题 11　(2016 年上半年试题 59)

使用 IEEE 802.1q 协议，最多可以配置__(59)__个 VLAN。

(59) A. 1022　　B. 1024　　C. 4094　　D. 4096

参考答案：(59)C。

要点解析：802.1q 的标识字段占 12 位，支持 4096 个 VLAN 的识别，但 0 用于识别帧的优先级，4095 作为预留值，故最多可配置 4094 个。

试题 12　(2016 年上半年试题 60)

VLAN 中继协议(VTP)有不同的工作模式，其中能够对交换机的 VLAN 信息进行添加、删除、修改等操作，并把配置信息广播到其他交换机上的工作模式是__(60)__。

(60) A. 客户机模式　　B. 服务器模式　　C. 透明模式　　D. 控制模式

参考答案：(60)B。

要点解析：VTP 有三种工作模式。

(1) 服务器模式：可以设置 VLAN 信息，服务器会自动将这些信息广播到网上的其他交换技术以统一配置。

(2) 客户模式：交换机不能配置 VLAN 信息，只能被动地接受服务器的 VLAN 配置。

(3) 透明模式：可以配置 VLAN 信息，但是不广播自己的 VLAN 信息，同时还可以接收服务器发来的 VLAN 信息后并不使用，而是直接转发给别的交换机。

试题 13　(2016 年上半年试题 61)

下面关于 VTP 的论述中，错误的是__(61)__。

(61) A. 静态修剪就是手工剪掉中继链路上不活动的 VLAN

B. 动态修剪使得中继链路上所有共享的 VLAN 都是活动的

C. 静态修剪要求在 VTP 域中的所有交换机都配置成客户机模式

D. 动态修剪要求在 VTP 域中的所有交换机都配置成服务器模式

参考答案：(61)C。

要点解析：静态修剪，就是手工剪掉中继链路上不活动的 VLAN。VTP 动态修剪允许交换机从中继连接上动态地剪掉不活动的 VLAN，使得所有共享的 VLAN 都是活动的。动态修剪的缺点是它要求在 VTP 域中的所有交换机都必须配置成服务器。

试题 14 (2016 年上半年试题 62)

IEEE 803.3ae 10Gb/s 以太网标准支持的工作模式是__(62)__。

(62) A. 单工　　B. 半双工　　C. 全双工　　D. 全双工和半双工

参考答案：(62)C。

要点解析：IEEE 803.3ae 标准支持 10Gb/s 的传输速率。传统以太网采用 CSMA/CD 协议，即带冲突检测的载波监听多路访问技术。万兆以太网与千兆以太网一样，基本上应用于点到点线路，但是不再共享带宽，只适用于全双工模式，不需要 CSMA/CD 协议支持。

试题 15 (2016 年上半年试题 63)

如图 3.7 所示，网桥 A、B、C 连接多个以太网。已知网桥 A 为根网桥，各个网桥的 a、b、f 端口为指定端口。那么按照快速生成树协议标准 IEEE 802.1d—2004，网桥 B 的 c 端口为__(63)__。

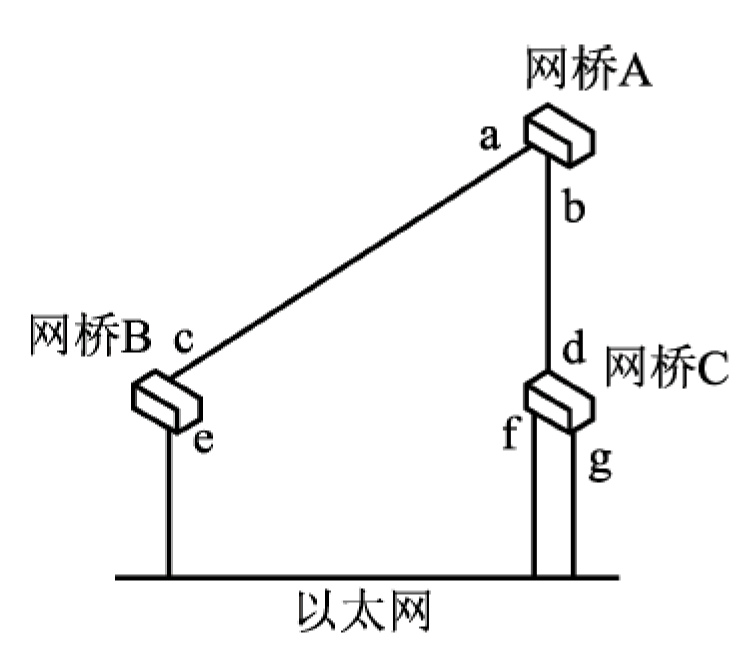


图 3.7　网桥连接

(63) A. 根端口(Root Port)　　B. 指定端口(Designated Port)
C. 备份端口(Backup Port)　　D. 替代端口(Alternate Port)

参考答案：(63)A。

要点解析：由于网桥 A 为根网桥，a、b、f 为指定端口，所以 c、d 端口为根端口(即通向根网桥的端口)。

试题 16 (2015 年下半年试题 12 和试题 13)

根据 STP 协议，网桥 ID 最小的交换机被选举为根网桥，网桥 ID 由__(12)__字节的优先级和 6 字节的__(13)__组成。

(12) A. 2　　B. 4　　C. 6　　D. 8

(13) A. 用户标识　　B. MAC 地址　　C. IP 地址　　D. 端口号

参考答案：(12) A；(13) B。

要点解析：网桥 ID 由交换机优先级(用 2 个字节表示，默认是 32768，最小的是 4096，



其他都是 4096 的倍数)和 MAC 地址(6 字节)组成。交换机的每个接口有一个 MAC 地址。

试题 17　(2015 年下半年试题 66)

用来承载多个 VLAN 流量的协议组是＿(66)＿。

(66) A. 802.11a 和 802.1q　　B. ISL 和 802.1q
C. ISL 和 802.3ab　　D. SSL 和 802.11b

参考答案：(66) B。

要点解析：在以以太网为介质的干道上，目前有两种主要的干道标记技术：国际标准 IEEE 802.1q 和思科的私有标准 ISL。

IEEE 802.1q 会在数据帧准备通过干道的时候对数据帧的帧头进行编辑，在数据帧的头上放置单一的标识，以标识数据帧来自哪个 VLAN。当数据帧离开干道时，标识被去除。

ISL 封装技术是思科公司开发的私有技术，在帧的前面和后面都添加封装信息，其中包含 VLAN ID。该封装协议在标准以太帧头部加上 26 字节的 ISL 头，在以太帧尾部加上 4 字节的 ISL 尾，共 30 个字节的封装信息。

试题 18　(2015 年上半年试题 22)

以下关于 VLAN 的叙述中，正确的是＿(22)＿。

(22) A. VLAN 对分组进行过滤，增强了网络的安全性
B. VLAN 提供了在大型网络中保护 IP 地址的方法
C. VLAN 在可路由的网络中提供了低延迟的互连手段
D. VLAN 简化了在网络中增加、移除和移动主机的操作

参考答案：(22) D。

要点解析：VLAN 技术的出现，使得管理员根据实际应用需求，把同一物理局域网内的不同用户逻辑地划分成不同的广播域，每一个 VLAN 都包含一组有着相同需求的计算机工作站，与物理上形成的 LAN 有着相同的属性。由于它是从逻辑上划分，而不是从物理上划分，所以同一个 VLAN 内的各个工作站没有限制在同一个物理范围中，即这些工作站可以在不同物理 LAN 网段。由 VLAN 的特点可知，一个 VLAN 内部的广播和单播流量都不会转发到其他 VLAN 中，从而有助于控制流量、减少设备投资、简化网络管理、提高网络的安全性。

试题 19　(2015 年上半年试题 23)

当局域网中更换交换机时，怎样保证新交换机成为网络中的根交换机？＿(23)＿

(23) A. 降低网桥优先级　　B. 改变交换机的 MAC 地址
C. 降低交换机端口的根通路费用　　D. 为交换机指定特定的 IP 地址

参考答案：(23) A。

要点解析：生成树协议根据网桥 ID 选举根交换机，网桥 ID 最小的交换机将被选为根网桥。网桥 ID 由网桥优先级和网桥 MAC 地址两部分组成，如果交换机的优先级相同则比较其 MAC 地址，地址值越小，其就被选举为根网桥。

试题 20　(2015 年上半年试题 33)

以下叙述中，不属于无源光网络优势的是＿(33)＿。

(33) A. 设备简单，安装维护费用低，投资相对较小
B. 组网灵活，支持多种拓扑结构
C. 安装方便，不用另外租用或建造机房
D. 无源光网络适用于点对点通信

参考答案：(33) D。

要点解析：无光源网络(Passive Optical Network, PON)是一种点对多点的光纤传输和接入技术，下行采用广播方式、上行采用时分多址方式，可以灵活地组成树型、星型、总线型等拓扑结构，在光分支点只需要安装一个简单的光分支器即可，因此具有节省光缆资源、带宽资源共享、节省机房投资、建网速度快、综合建网成本低等优点。无源光网络包括ATM-PON 和 Ethernet-PON 两种。

试题 21 (2015 年上半年试题 60)

以太网采用物理地址的目的是 (60) 。

(60) A. 唯一地标识第二层设备
B. 使用不同网络中的设备可以互相通信
C. 用于区分第二层的帧和第三层的分组
D. 物理地址比网络地址的优先级高

参考答案：(60) A。

要点解析：MAC(Media Access Control)地址也称为物理地址、硬件地址，用来定义网络设备的位置。在 OSI 模型中，第三层网络层负责 IP 地址，第二层数据链路层则负责 MAC 地址。

3.4 强化训练

3.4.1 综合知识试题

试题 1 (2014 年下半年试题 26 和试题 27)

城域以太网在各个用户以太网之间建立多点第二层连接，IEEE 802.1ah 定义的运营商主干网协议提供的基本技术是在用户以太帧中再封装一层 (26) ，这种技术被称为 (27) 技术。

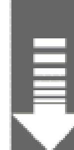
(26) A. 运营商的 MAC 帧头　　B. 运营商的 VLAN 标记
C. 用户 VLAN 标记　　D. 用户帧类型标记

(27) A. Q-in-Q　　B. IP-in-IP　　C. NAT-in-NAT　　D. MAC-in-MAC

试题 2 (2014 年下半年试题 63)

在局域网中可动态或静态划分 VLAN，静态划分 VLAN 是根据 (63) 划分。

(63)A. MAC 地址　　B. IP 地址　　C. 端口号　　D. 管理区域



试题 3　(2014 年上半年试题 23)

动态划分 VLAN 的方法中不包括__(23)__。

(23) A. 网络层协议　B. 网络层地址　C. 交换机端口　D. MAC 地址

试题 4　(2014 年上半年试题 24 和试题 25)

在局域网中划分 VLAN，不同 VLAN 之间必须通过__(24)__才能互相通信，属于各个 VLAN 的数据帧必须打上不同的__(25)__。

(24) A. 中继端口　B. 动态端口　C. 接入端口　D. 静态端口

(25) A. VLAN 优先级　B. VLAN 标记　C. 用户标识　D. 用户密钥

试题 5　(2014 年上半年试题 26 和试题 27)

城域以太网在各个用户以太网之间建立多点第二层连接，IEEE 802.1ad 定义的运营商网桥协议提供的基本技术是在以太帧中插入__(26)__字段，这种技术被称为__(27)__技术。

(26) A. 运营商 VLAN 标记　B. 运营商虚电路标识
C. 用户 VLAN 标记　D. 用户帧类型标记

(27) A. Q-in-Q　B. IP-in-IP　C. NAT-in-NAT　D. MAC-in-MAC

试题 6　(2014 年上半年试题 50)

某实验室使用无线路由器提供内部上网，无线路由器采用固定 IP 地址连接至校园网，实验室用户使用一段时间后，不定期出现不能访问互联网的现象，经测试无线路由器工作正常，同时有线接入的用户可以访问互联网。分析以上情况，导致这一故障产生的最可能的原因是__(50)__。

(50) A. 无线路由配置错误　B. 无线路由器硬件故障
C. 内部或者外部网络攻击　D. 校园网接入故障

3.4.2　综合知识试题参考答案

【试题 1】答　案：(26)A；(27)D。

解　析：MAC-in-MAC 封装又称网络提供商骨干桥(PBB)技术，遵循 IEEE 802.1ah 标准。其基本思路是将用户的以太网数据帧再封装一个运营商的以太网帧头，形成两个 MAC 地址。

【试题 2】答　案：(63)C。

解　析：许多 VLAN 厂商都利用交换机的端口来划分 VLAN 成员。被设定的端口都在同一个广播域中，属于静态划分。

根据 MAC 地址划分 VLAN 的方法是根据每个主机的 MAC 地址来划分的，即对每个 MAC 地址的主机都配置它属于哪个组，属于动态划分。

【试题 3】答　案：(23)C。

解　析：在交换机上实现 VLAN，可以采用静态的或动态的方法。

① 静态分配 VLAN：为交换机的各个端口指定所属的 VLAN。这种基于端口的划分方法是把各个端口固定地分配给不同的 VLAN，任何连接到交换机的设备都属于接入端口

所在的 VLAN。

② 动态分配 VLAN：动态 VLAN 通过网络管理软件包来创建，可以根据设备的 MAC 地址、网络层协议、网络层地址、IP 广播域或管理策略来划分 VLAN。根据 MAC 地址划分 VLAN 的方法应用最多，一般交换机都支持这种方法。无论一台设备连接到交换网络的任何地方，接入交换机根据设备的 MAC 地址就可以确定该设备的 VLAN 成员身份。这种方法使得用户可以在交换网络中改变接入位置，而仍能访问所属的 VLAN。

但是当用户数量很多时，对每个用户设备分配 VLAN 的工作量是很大的管理负担。

【试题 4】答　案：(24)A；(25)B。

解　析：在划分成 VLAN 的交换网络中，交换机端口之间的连接分为两种：接入链路连接)和中继链路连接。接入链路只能连接具有标准以太网卡的设备，也只能传送属于单个 VLAN 的数据包。中继链路是在一条物理连接上生成多个逻辑连接，每个逻辑连接属于一个 VLAN。在进入中继端口时，交换机在数据包中加入 VLAN 标记。

【试题 5】答　案：(26)A；(27)A。

解　析：Q-in-Q 技术(也称 Stacked VLAN 或 Double VLAN)。标准出自 IEEE 802.1ad，其实现将用户私网 VLAN Tag 封装在公网 VLAN Tag 中，使报文带着两层 VLAN Tag 穿越运营商的骨干网络(公网)。其实现为在 802.1q 协议标签前再次封装 802.1q 协议标签，其中一层标识用户系统网络(Customer Network)，一层标识网络运营商网络(Service Provider Network)，将其扩展实现用户线路标识。

【试题 6】答　案：(50)C。

解　析：路由器工作正常以及有线环境的用户访问互联网正常，可以排除无线路由器硬件故障和校园网接入故障的因素。另外，题干中明确指出实验室用户可以访问互联网，证明无线路由器配置无误。至于出现不定期不能访问互联网的现象，据推测可能是内部 ARP 攻击或来自外部网络的攻击。

第 4 章 无线通信网

4.1 备考指南

4.1.1 考纲要求

根据考试大纲中相应的考核要求，在“无线通信网”知识模块上，要求考生掌握以下方面的内容。

(1) 移动通信：蜂窝系统的原理，第二代移动通信技术 GSM 和 CDMA，第三代移动通信技术 CDMA 2000、WCDMA 和 TD-SCDMA。

(2) 无线局域网：无线接入点 AP 和 Ad Hoc 网络，扩频通信技术 DSSS 和 HFSS，CSMA/CA 协议，802.11a/802.11b/802.11g 标准，认证技术 WEP 和 802.11i。

(3) 无线个域网：蓝牙技术和 ZigBee。

(4) 无线城域网：无线城域网关键技术、WiMAX 技术、802.16e。

4.1.2 考点统计

“无线通信网”知识模块在历次网络工程师考试试卷中出现的考核知识点及分值分布情况如表 4.1 所示。

表 4.1 历年考点统计表

年 份	题 号	知 识 点	分 值
2017 年下半年	上午：44、57	WLAN、CSMA/CD 协议	7 分
	下午：无	无	0 分
2017 年上半年	上午：34、64、66	CSMA/CD 协议、IEEE 802 标准	3 分
	下午：无	无	0 分

续表

年 份	题 号	知 识 点	分 值
2016 年下半年	上午：65～67	WLAN、CSMA/CD 协议、IEEE 802 标准	3 分
	下午：无	无	0 分
2016 年上半年	上午：65、66	CSMA/CD 协议	1 分
	下午：无	无	0 分
2015 年下半年	上午：62、64、65	CSMA/CD 协议、4G 技术	3 分
	下午：无	无	0 分
2015 年上半年	上午：49、50、62、63	IEEE 802.1x 协议、WPA 安全认证方案、4G 通信技术、移动 Ad Hoc 网络	4 分
	下午：无	无	0 分
2014 年下半年	上午：47、62、64、65	无线接入点、WLAN 通信技术、ZigBee 网络	4 分
	下午：无	无	0 分
2014 年上半年	上午：60～63	3G 通信标准、IEEE 802.11 标准、Ad Hoc 网络	4 分
	下午：无	无	0 分
2013 年下半年	上午：66、67	IEEE 802.11 标准	2 分
	下午：无	无	0 分
2013 年上半年	上午：60、66	CSMA/CA 协议、Wi-Fi 安全协议	2 分
	下午：无	无	0 分
2012 年下半年	上午：64～66	CSMA/CA 协议、无线传感技术、无线通信技术	3 分
	下午：无	无	0 分
2012 年上半年	上午：65～67	无线接入点和 IEEE 802.11n、IEEE 802.16 提出的 WiMAX	3 分
	下午：无	无	0 分

4.1.3 命题特点

2014 年出版的《网络工程师(第 4 版)》将无线通信从“局域网和城域网”中分离出来作为单独的一章，并添加了移动通信、无线局域网和无线城域网等当前主流技术。2014 年两次考试中已出现了相关的题目，新加的内容需要作为学习的重点。

无线局域网标准和 CSMA/CA 协议是重点，一般考试中都会出现。

4.2 考点串讲

4.2.1 移动通信

4.2.1.1 蜂窝通信系统

蜂窝系统也叫“小区制”系统，如图 4.1 所示，它将所有要覆盖的地区划分为若干小区，每个小区的半径可视用户的分布密度为 1～10km，形成了形状酷似“蜂窝”的结构，因而把这种移动通信方式称为蜂窝移动通信方式。在每个小区设立一个基站为本小区范围内的



用户服务，并可通过小区分裂进一步提高系统容量。相邻小区不能使用相同的频率通信。当用户移动到一个小区的边缘时，电话信号的衰减程度提醒相邻的基站进行切换操作，正在通信的用户就自动切换到另一个小区的频段继续通话。

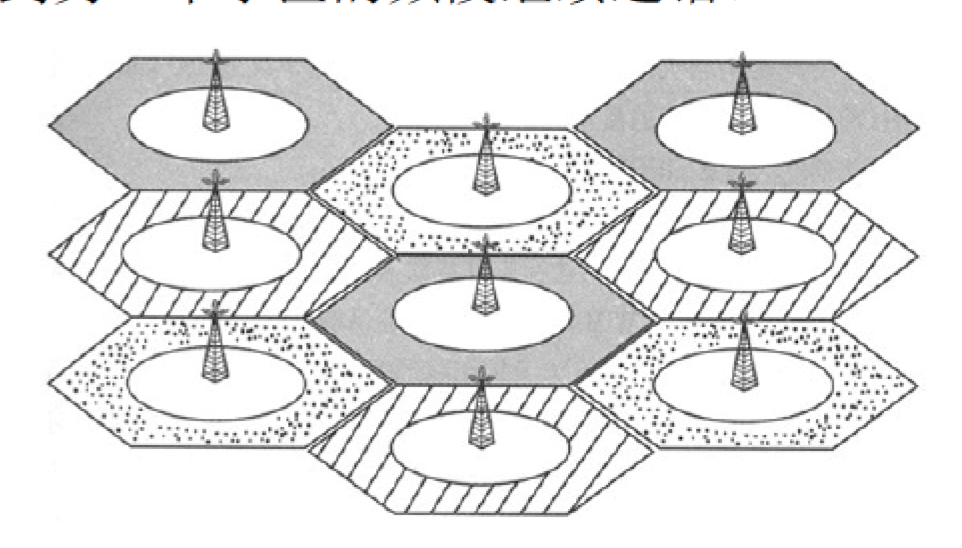


图 4.1　蜂窝通信系统

4.2.1.2　第二代移动通信系统

第二代移动通信系统是引入数字无线电技术组成的数字蜂窝移动通信系统，它提供更高的网络容量，改善了话音质量和保密性，并为用户提供无缝的国际漫游。在中国，第二代移动通信系统以 GSM 为主，以 CDMA 为辅。

1. GSM

GSM 全称为 Global System for Mobile Communications，中文为全球移动通信系统。目前，中国移动、中国联通各拥有一个 GSM 网，为世界最大的移动通信网络。GSM 系统包括 GSM 900——900MHz、GSM1800——1800MHz 及 GSM1900——1900MHz 等几个频段。

2. CDMA

美国高通公司的第二代数字蜂窝移动通信系统工作在 800MHz 频段，采用码分多址 CDMA 技术提供话音和数据业务。

CDMA 系统是基于码分技术(扩频技术)和多址技术的通信系统，它为每个用户分配各自特定地址码。地址码之间具有相互准正交性，从而在时间、空间和频率上都可以重叠；将需传送的具有一定信号带宽的信息数据，用一个带宽远大于信号带宽的伪随机码进行调制，使原有的数据信号的带宽被扩展，接收端进行相反的过程，进行解扩，增强了抗干扰的能力。

3. 2.5G

2.5G 移动通信技术是从 2G 迈向 3G 的衔接性技术，由于 3G 是个相当浩大的工程，所牵扯的层面多且复杂，要从 2G 迈向 3G 不可能一下就衔接得上，因此出现了介于 2G 和 3G 之间的 2.5G。GPRS、HSCSD、WAP、EDGE、蓝牙(Bluetooth)、EPOC 等技术都是 2.5G 技术。

4.2.1.3　第三代移动通信系统

3G 是第三代移动通信技术，是指支持高速数据传输的蜂窝移动通信技术。3G 服务能够同时传送声音及数据信息，下行速度峰值理论可达 3.6Mb/s(一说 2.8Mb/s)，上行速度峰值也可达 384Kb/s。

中国国内支持国际电联确定三个无线接口标准，分别是中国电信的 CDMA 2000、中国

联通的WCDMA、中国移动的TD-SCDMA。GSM设备采用的是时分多址，而CDMA使用码分扩频技术，先进功率和话音激活至少可提供大于3倍的GSM网络容量，业界将CDMA技术作为3G的主流技术。国际电联确定三个无线接口标准，分别是美国CDMA 2000、欧洲WCDMA、中国TD-SCDMA。原中国联通的CDMA卖给中国电信，中国电信已经将CDMA升级到3G网络，3G的主要特征是可提供移动宽带多媒体业务。

4.2.2 无线局域网

4.2.2.1 无线局域网的基本概念

1. 无线局域网协议体系

(1) IEEE 802.11协议标准体系：由面向数据通信的计算机局域网发展而来的，采用的是无连接协议。

(2) HIPERLAN协议标准体系：由欧洲邮电委员会(CEPT)制定的，致力于面向语音的蜂窝电话，采用的是基于连接的协议。

2. 802.11标准

IEEE 802.11委员会相继制定了多种物理层标准。1997年颁布的IEEE 802.11标准运行在2.4GHz的ISM段频，采用扩频通信技术，支持1Mb/s和2Mb/s数据速率。随后又出现了两个新的标准，1998年推出IEEE 802.11b标准，也是运行在ISM频段，采用CCK技术，支持11Mb/s的数据速率。1999年推出的IEEE 802.11a标准运行在U-NII频段，采用OFDM调制技术，支持最高达54Mb/s的数据速率。目前的WLAN标准主要有4种，如表4.2所示。

表4.2 IEEE 802.11标准

名 称	发布时间	工作频段	调制技术	数据速率
802.11	1997年	2.4GHz ISM频段	DBPSK	1Mb/s
			DQPSK	2Mb/s
802.11b	1998年	2.4GHz ISM频段	CCK	5.5Mb/s、11Mb/s
802.11a	1999年	5GHz U-NII频段	OFDM	54Mb/s
802.11g	2003年	2.4GHz ISM频段	OFDM	54Mb/s

3. WLAN的拓扑结构

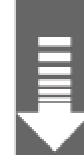
IEEE 802.11标准定义了两种无线网络的拓扑结构，一种是基础设施网络(Infrastructure Networking)，另一种是特殊网络(Ad Hoc Networking)。

在基础设施网络中，无线终端通过接入点访问骨干网设备，或者相互访问。

Ad Hoc网络是一种点对点连接，不需要有线网络和接入点的支持，以无线网卡连接的终端设备之间可以直接通信。这种拓扑结构适合在移动情况下快速部署网络，主要用在军事领域，也可以用在商业领域进行语音和数据传输。

4.2.2.2 WLAN的通信技术

现在无线网主要使用3种通信技术：红外线、扩展频谱和无线电技术。这三种技术的



主要特点如表 4.3 所示。

表 4.3　WLAN 通信技术的比较

项　目	红 外 线		扩展频谱		无 线 电
	散射红外线	定向红外光束	频率跳动	直接序列	窄带微波
数据速率(Mb/s)	1～4	10	1～3	2～20	5～10
移动特性	固定/移动	与 LOS 固定	移动	固定/移动	
范围(ft)	50～200	80	100～300	100～800	40～130
可监测性	可忽略		几乎无		有一些
波长/频率	λ为 850～950nm		ISM 频带：902M～928MHz、2.4G～2.4835GHz、5.725G～5.875GHz		18.825G～19.025GHz 或 ISM 频带
调制技术	OOK		GFSK	QPSK	FSK/QPSK
辐射能量	NA		<1W		25mW
访问方法	CSMA	令牌环，CSMA	CSMA		预约 ALOHA，CSMA
需许可证否	否		否		除 ISM 外都要

4.2.2.3　IEEE 802.11 WLAN 体系结构

802.11 WLAN 的协议体系结构如图 4.2 所示。其中 LLC 子层与以太网一样都是 IEEE 802.2。

数据链路层	LLC		站管理
	MAC	MAC 管理	
物理层	PLCP	PHY 管理	
	PMD		

图 4.2　WLAN 体系结构

MAC 层分为 MAC 子层和 MAC 管理子层。MAC 子层负责访问和分组拆装，MAC 管理子层负责 ESS 漫游、电源管理和登记过程中的关联管理。物理层分为物理层汇聚协议(Physical Layer Convergence Protocol，PLCP)、物理介质相关(Physical Medium Dependent，PMD)子层和 PHY 管理子层。PLCP 主要进行载波监听和物理层分组的建立，PMD 用于传输信号的调制和编码，而 PHY 管理子层负责选择物理信道和调谐。

1. *物理层*

IEEE 802.11 定义了 3 种 PLCP 帧格式来对应 3 种不同的 PMD 子层通信技术。

1)　FHSS

对应于 FHSS 通信的 PLCP 帧格式如图 4.3 所示。

SYNC(80)	SFD(16)	PLW(12)	PSF(4)	CRC(16)	MPDU(≤4096 字节)

图 4.3　用于 FHSS 方式的 PLCP 帧

SYNC 是 0 和 1 的序列，共 80 比特作为同步信号。SFD 的比特模式为 0000110010111101，用作帧的起始符。PLW 代表帧的长度，共 12 位，所以帧最大长度可以达到 4096 字节。PSF 是分组信令字段，用来标识不同的数据速率。起始数据速率为 1Mb/s，以 0.5 的步长递增。PSF=0000 时代表数据速率为 1Mb/s，PSF 为其他数值时则在起始速率的基础上增加一定倍数的步长，例如 PSF=0010，则 1Mb/s+0.5Mb/s×2=2Mb/s。16 位的 CRC 是为了保护 PLCP

头部所加的，它能纠正2比特错误。MPDU代表MAC协议数据单元。

2) DSSS

图4.4所示为采用DSSS通信时的帧格式。

与前一种不同的字段解释如下：SFD字段的比特模式为1111001110100000。Signal字段表示数据速率，步长为100Kb/s，比FHSS精确5倍。Service字段保留未用。Length字段指MPDU的长度。FCS则是帧校验序列。

SYNC(128)	SFD(16)	Signal(8)	Service(8)	Length(16)	FCS(8)	MPDU

图4.4　用于DSSS方式的PLCP帧

3) DFIR

图4.5所示为采用漫反射红外线时的PLCP帧格式。

SYNC(57－73)	SFD(4)	Data rate(3)	DCLA(32)	Length(16)	FCS(16)	MPDU

图4.5　用于DFIR方式的PLCP帧

DFIR的SYNC比FHSS和DSSS的都短，因为采用光敏二极管检测信号不需要复杂的同步过程。Data rate字段=000，表示1Mb/s，Data rate字段=001，表示2Mb/s。DCLA是直流电平调节字段，通过发送32个时隙的脉冲序列来确定接收信号的电平。MPDU的长度不超过2500字节。

2. 802.11 MAC子层

802.11标准为MAC子层定义了3种访问控制机制：一是通过CSMA/CA方式进行分布式协调功能DCF，用于支持争用服务；二是通过点协调功能(PCF)来支持无争用服务；三是通过RST/CST来支持信道预约。图4.6所示是DCF和PCF之间的关系。

1) CSMA/CA协议

其原理如图4.7所示。

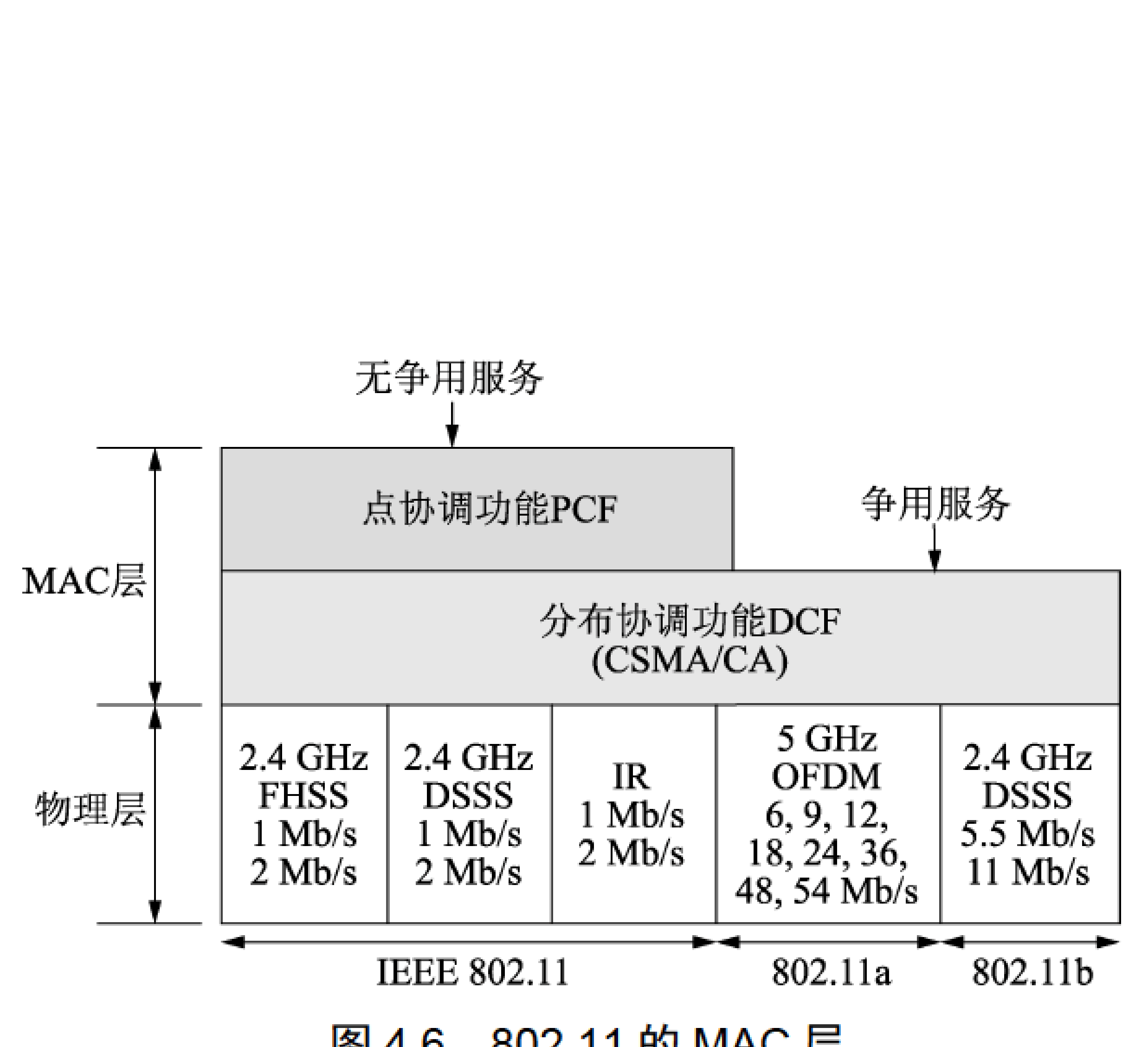


图4.6　802.11的MAC层

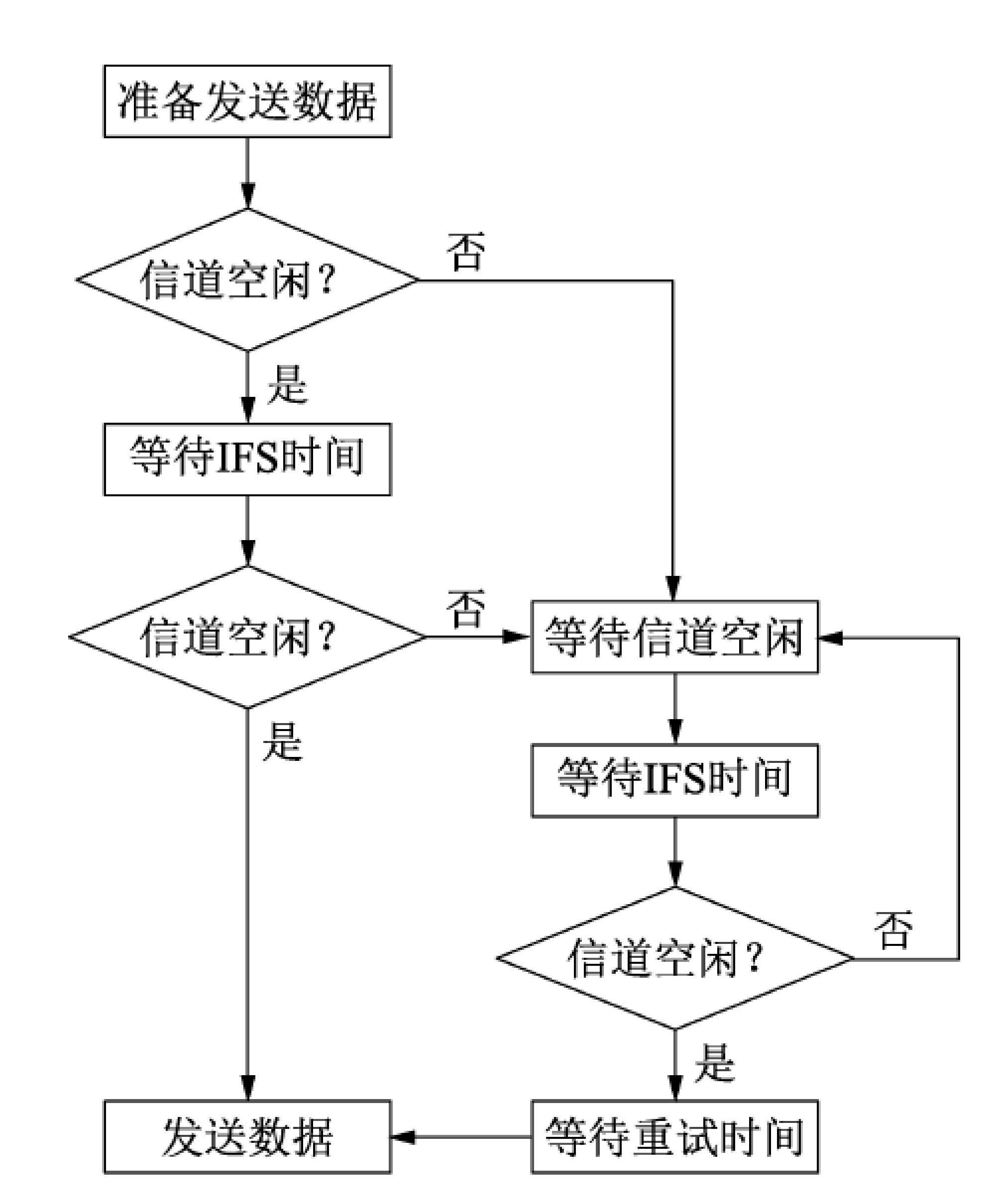


图4.7　CSMA/CA协议的工作原理



为了尽量避免碰撞，所有的站在完成发送后，必须再等待一段很短的时间(继续监听)才能发送下一帧。这段时间的通称是帧间间隔 IFS，有三种帧间间隔。

- SIFS：短(Short)帧间间隔，长度为 28 μs，是最短的帧间间隔，用来分隔属于一次对话的各帧。
- PIFS：点协调功能帧间间隔(比 SIFS 长)，是为了在开始使用 PCF 方式时(在 PCF 方式下使用，没有争用)优先获得接入到媒体中。PIFS 的长度是 SIFS 加一个时隙(Slot)长度(其长度为 50 μs)，即 78 μs。
- DIFS：分布协调功能帧间间隔(最长的 IFS)，在 DCF 方式中用来发送数据帧和管理帧。DIFS 的长度比 PIFS 再增加一个时隙长度，因此 DIFS 的长度为 128 μs。

2)　分布式协调 DCF

802.11 MAC 层定义的分布式协调功能(Distributed Coordination Function，DCF)利用了 CSMA/CA 协议，在此基础上又定义了点协调功能(Point Coordination Function，PCF)。DCF 是数据传输的基本方式，作用于信道竞争期。PCF 工作于非竞争期。两者总是交替出现，先由 DCF 竞争介质使用权，然后进入非竞争期，由 PCF 控制数据传输。

3)　点协调 PCF

PCF 是在 DCF 之上实现的一个可选功能，在 Ad Hoc 网络中没有 PCF。它由 AP 集中轮询所有移动站，将发送数据权轮流交给各个站，从而避免了碰撞的产生，为它们提供无争用服务。这种机制适用于对时间敏感的业务，如分组话音等。轮询过程中使用 PIFS 作为帧间隔时间。由于 PIFS 比 DIFS 小，所以点协调能够优先 CSMA/CA 获得信道，并把所有的异步帧都推后传送。

3. MAC 管理子层

WLAN 是开放系统，各站点共享传输介质，而且通信站具有移动性，因此，必须解决信息的同步问题、漫游问题、保密问题和节能问题。

1)　同步问题

信标是一种管理帧，由 AP 定期发送，用于进行时间同步。同步方式有主动扫描和被动扫描两种。

所谓主动扫描，就是终端在预定的各个频道上连续扫描，发射探试请求帧，并等待各个 AP 回答的响应帧；收到各 AP 的响应帧后，工作站将对各个帧中的相关部分进行比较以确定最佳 AP。

终端获得同步的另一种方法是被动扫描。如果终端已在 BSS 区域，那么它可以收到各个 AP 周期性发射的信标帧，因为帧中含有同步信息，所以工作站对各帧进行比较后，确定最佳 AP。

2)　移动方式

IEEE 802.11 定义了 3 种移动方式：无转移方式、BSS 转移和 ESS 转移。

- 无转移方式是指终端是固定的，或者仅在 BSA 内部移动。
- BSS 转移是指终端在同一 ESS 内部的多个 BSS 之间移动。
- ESS 转移是指从一个 ESS 移动到另一个 ESS。

3)　安全管理

为了达到与有线网络同等的安全性能，IEEE 802.11 采取了认证和加密措施。

IEEE 802.11 提供的加密方式采用有线等价协议(Wired Equivalency Protocol，WEP)。WEP 是一种对称性的加密技术，即加密和解密都使用同样的算法和密钥，其加密算法是 RC4 流加密协议，密钥长度最初为 40 位(5 个字符)，后来增加到 128 位(13 个字符)。使用静态 WEP 加密可以设置 4 个 WEP Key，使用动态 WEP 加密时，WEP Key 会随时间变化而变化。

2004 年 6 月公布的 IEEE 802.11i 标准是对 WEP 协议的改进。802.11i 定义了新的密钥交换协议(Temporal Key Integrity Protocol，TKIP)和高级加密标准(Advanced Encryption Standard，AES)。TKIP 提供了报文完整性检查，每个数据包使用不同的混合密钥(per-packet key mixing)，每次建立连接时生成一个新的基本密钥(re-keying)，这些手段的使用使得诸如密钥共享、碰撞攻击和重放攻击等无能为力，从而减少了 WEP 协议的安全隐患。

4) 电源管理

IEEE 802.11 允许空闲站处于睡眠状态，在同步时钟的控制下周期性地唤醒处于睡眠态的空闲站，由 AP 发送的信标帧中的 TIM(业务指示表)指示是否有数据暂存于 AP，若有，则向 AP 发探询帧，从 AP 接收数据，然后进入睡眠态；若无，则立即进入睡眠态。

4.2.2.4 移动 Ad Hoc 网络

与传统的有线网络相比，MANET 有以下特点。

- 网络拓扑结构是动态变化的。
- 无线信道提供的带宽较小，而信号衰落和噪声干扰的影响却很大。
- 无线终端携带的电源能量有限。
- 由于无线链路的开放性，容易招致网络窃听、欺骗、拒绝服务等恶意攻击的威胁。
- 无线移动自组织网络中还有一种特殊的现象，这就是隐蔽终端和暴露终端问题。

1. MANET 中的路由协议

根据路由策略可分为表驱动的路由协议和源路由协议；根据网络结构可以划分为扁平的路由协议、分层的路由协议和基于地理信息的路由协议。表驱动路由和源路由都是扁平的路由协议。

根据设计原理，扁平的路由协议还可进一步划分为先验式(表驱动)路由和反应式(按需分配)路由，前者大部分是基于链路状态算法的，而后者主要是基于距离矢量算法的。

先验式(Proactive)路由是表驱动型协议，通过周期地交换路由信息，每个节点可以保存完整的网络拓扑结构图，因而可以主动确定网络布局。按需分配的路由协议提供了可伸缩的路由解决方案。其主要思想是，移动节点只是在需要通信时才发送路由请求分组，以此来减少路由开销。

当网络规模扩大时，扁平路由协议产生的路由开销迅速增大，先验式路由会由于周期性交换各链路状态信息而消耗太多的带宽，即使反应式路由，也会由于越来越长的数据通路需要频繁维护而产生过多的控制开销。在这种情况下，采用分层的方案是一种较好的选择。

地理信息路由协议要求所有的节点都必须及时地访问地理坐标系统。例如，地理寻址路由协议。

2. DSDV 协议

DSDV(Destination-Sequenced Distance Vector，目标排序的距离矢量)协议是由 Perkins



和 P. Bhagwat 于 1994 年提出的一种基于 Bellman-Ford 算法的表驱动路由方案。DSDV 是一种扁平式路由协议。DSDV 的路由表项中包含目标地址、下一跳地址、跳步数、序列号、安装时间、稳定数据等字段。

DSDV 节点周期性地广播路由公告，但是在出现新链路或者老链路断开时立即触发链路公告。

当一个节点接收到邻居节点发送的路由公告时，根据下列规则进行路由更新：对应于某个标的路由表项，如果收到的序列号比路由表中已有的序列号更大，则更新现有的路由表项；如果收到的序列号和现有的序列号相同，但度量值更小，也要更新现有的路由表项；否则放弃收到的路由更新公告，维持现有的路由表项不变。

通过序列号机制可以排除路由环路现象，但 DSDV 要解决路由波动问题。为了解决这个问题，DSDV 采用平均定制时间(Average Setting Time，AST)来决定发布路由公告的时间间隔，AST 表示对应目标节点更新路由的平均时间间隔，而最近定制时间(Last Setting Time，LST)则是最近一次更新路由的时间间隔。第 n 次的平均定制时间是最近定制时间与前 $n-1$ 次的平均定制时间的加权平均值，即

$$\text{AST}_n = \frac{2\text{LST} + \text{AST}_{n-1}}{3}$$

为了减少路由波动，节点可以等待两倍的 AST_n 时间再发送路由公告。

3. AODV 协议

按需分配的距离矢量协议(Ad hoc On-Demand Distance Vector，AODV)也是一种扁平式路由协议，但是采用了反应式路由策略。

AODV 采用了类似于 DSDV 的序列号机制，用于排除一般距离矢量协议可能引起的路由环路问题。AODV 的路由表项由下列字段组成：目标 IP 地址、目标子网掩码、目标序列号、下一跳 IP 地址、路由表项的生命周期、度量值/跳步数、网络接口、其他的状态和路由标识。

AODV 是一种按需路由协议。当一个节点需要给网络中的其他节点传送信息时，如果没有到达目标节点的路由，则必须先以多播的形式发出 RREQ(路由请求)报文。

当一个节点接收到 RREQ 请求时，如果它就是请求的目标，或者知道到达目标的路由并且其中的目标序列号大于 RREQ 中的目标序列号，则要响应这个请求，向发送 RREQ 的节点返回(单播)一个路由应答(Route Reply，RREP)报文。如果收到 RREQ 报文的节点不知道该目标的路由，则它要重新广播 RREQ 请求，并且记录发送 RREQ 报文的节点 IP 地址及其广播序列号(RREQ ID)。如果收到的 RREQ 报文已经被处理过了，则丢弃该报文，不再进行转发。

AODV 协议也适用于组播网络。

4.2.2.5　IEEE 802.11 的新进展

无线局域网面临两个主要问题，一是增强安全性，二是提高数据速率。

1. WLAN 的安全

1)　SSID 访问控制

可以对各个无线接入点(AP)设置不同的 SSID(Service Set Identifier)，当然，也可以禁用

SSID 广播。

2) 物理地址过滤

在无线路由器中维护一组允许访问的 MAC 地址列表，用于实现物理地址过滤功能。

3) 有线等效保密

有线等效保密(Wired Equivalent Privacy，WEP)使用 RC4 协议进行加密，并使用 CRC-32 校验保证数据的正确性。最初的 WEP 标准使用 24 位的初始向量，加上 40 位的字符串，构成 64 位的 WEP 密钥。后来美国政府放宽了出口密钥长度的限制，允许使用 104 位的字符串，加上 24 位的初始向量，构成 128 位的 WEP 密钥。

4) WPA

Wi-Fi 联盟的厂商们以 802.11i 草案的一个子集为蓝图制定了称为 WPA(Wi-Fi Protected Access)的安全认证方案。在 WPA 的设计中包含了认证、加密和数据完整性校验 3 个组成部分。

首先是 WPA 使用了 802.1x 协议对用户的 MAC 地址进行认证；其次是 WEP 增大了密钥和初始向量的长度，以及 128 位的密钥和 48 位的初始向量(IV)用于 RC4 加密。WPA 还采用了可以动态改变密钥的临时密钥完整性协议(Temporary Key Integrity Protocol，TKIP)，通过更频繁地变换密钥来减少安全风险。

5) IEEE 802.11i

IEEE 802.11i 标准包含以下两个方面的安全部件。

- 临时密钥完整性协议(TKIP)是一个短期的解决方案，仍然使用 RC4 加密方法，但是弥补了 WEP 的安全缺陷。
- 重新制定了新的加密协议，称为 CBC-MAC 协议的计时器模式(Counter Mode with CBC-MAC Protocol，CCMP)。这是基于高级加密标准(Advanced Encryption Standard，AES)的加密方法。

采用802.1x进行身份认证。如果认证通过，则AP为无线工作站打开一个逻辑端口。

可扩展的认证协议(Extensible Authentication Protocol，EAP)是一种专门用于认证的传输协议，常用的认证机制有 EAP-MD5、Lightweight EAP (LEAP)、EAP-TLS。

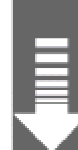
802.11i 还提供了一种任选的加密方案 WRAP(Wireless Robust Authentication Protocol)，实现了一种动态密钥交换和管理体制。对于小型办公室和家庭应用，可以使用预共享密钥(Pre-Shared Key，PSK)的方案，这样就可以省去 802.1x 认证和密钥交换过程了。

2. WLAN 的传输速率

2009 年 9 月 11 日，IEEE 802.11n 标准正式发布。802.11n 结合了 MIMO 与 OFDM 技术，可以将 WLAN 的传输速率由 802.11a/802.11g 的 54Mb/s 提高到 300Mb/s，甚至 600Mb/s。

正交频分复用(Orthogonal Frequency Division Multiplexing，OFDM)是一种多载波调制技术。其主要思想是将信道划分成若干正交子信道，将高速数据信号转换成并行的低速子数据流，并将各个子数据流交织编码，调制到正交的子信道上进行传输，在接收端采用相关技术可以将正交信号再分开。OFDM 具有较高的频谱利用率。

MIMO(Multiple Input Multiple Output，多入多处)是通过多径无线信道实现的，传输的信息流经过空时编码成 N 个子信息流，由 N 个天线发射出去，经空间信道传输后由 M 个接收天线接收。多天线接收机利用先进的空时编码处理功能对数据流进行分离和解码，从而



实现最佳的处理结果。

4.2.3　无线个域网

1998 年，IEEE 802.15 工作组成立，专门从事 WPAN 标准化工作。它的任务是开发一套适用于短程无线通信的标准，通常我们称之为无线个人局域网(WPAN)。

目前，IEEE 802.15 WPAN 共拥有 4 个工作组。

- 蓝牙 WPAN 工作组(802.15.1)：蓝牙是无线个人局域网的先驱。在初始阶段，IEEE 并没有制定蓝牙的相关标准，所以经过一段快速发展时期后，蓝牙很快就有了产品兼容性的问题。现在，IEEE 决定制定行业标准来开发能够相互兼容的蓝牙芯片、网络和产品。
- 共存组(802.15.2)：为所有工作在 2.4GHz 频带上的无线应用建立一个标准。
- 高数据率 WPAN 工作组(802.15.3)：其 802.15.3 标准适用于高质量要求的多媒体应用领域。
- 802.15.4 工作组(802.15.4)：为了满足低功耗、低成本的无线网络要求，IEEE 标准委员会在 2000 年 12 月正式批准并成立了 802.15.4 工作组，其任务就是开发一个低数据率的 WPAN(LR-WPAN)标准。它具有复杂度低、成本极少、功耗很小的特点，能在低成本设备(固定、便携或可移动的)之间进行低数据率的传输。

4.2.3.1　蓝牙技术

Bluetooth 无线技术是一种短距离通信技术，旨在取代电缆来连接便携式和/或固定设备，并保证高度安全性。Bluetooth 技术的主要特点在于功能强大、耗电量低、成本低廉。Bluetooth 规格为广泛范围的设备定义了统一的结构，以便于彼此之间进行连接和通信。

Bluetooth 技术已获得了全球认可，世界各地的 Bluetooth 设备都可以与其邻近的 Bluetooth 设备连接。Bluetooth 电子设备可以通过短距离的即时网络(称为微微网)进行无线连接和通信。每个设备最多可以在微微网中同时与七个其他设备进行通信。每个设备还可以同时属于多个微微网。当 Bluetooth 设备进入或撤离无线邻近区域时，微微网可在此期间自动动态建立。

Bluetooth 无线技术的基本优势在于它可以同时处理数据和语音传输。这使得用户可以享受各种创新解决方案，如免提耳机接听语音电话、打印和传真功能、同步 PDA、膝上型计算机和手机应用程序等。

1. 核心系统体系结构

蓝牙核心系统的体系结构如图 4.8 所示。

最下面的 Radio 层相当于 OSI 的物理层，其中的 RF 模块采用 2.4GHz 的 ISM 频段实现跳频通信(FHSS)，信号速率为 1Mb/s，数据速率为 1Mb/s。物理信道被划分为时槽，数据被封装成分组，每个分组占用一个时槽。在一对收发设备之间可以用时分多路(TTD)方式实现全双工通信。

物理信道之上是各种链路和信道层及其有关的协议。以物理信道为基础，向上依次形成的信道层次为物理信道、物理链路、逻辑传输、逻辑链路和 L2CAP (Logical Link Control

and Adaptation Protocol)信道。

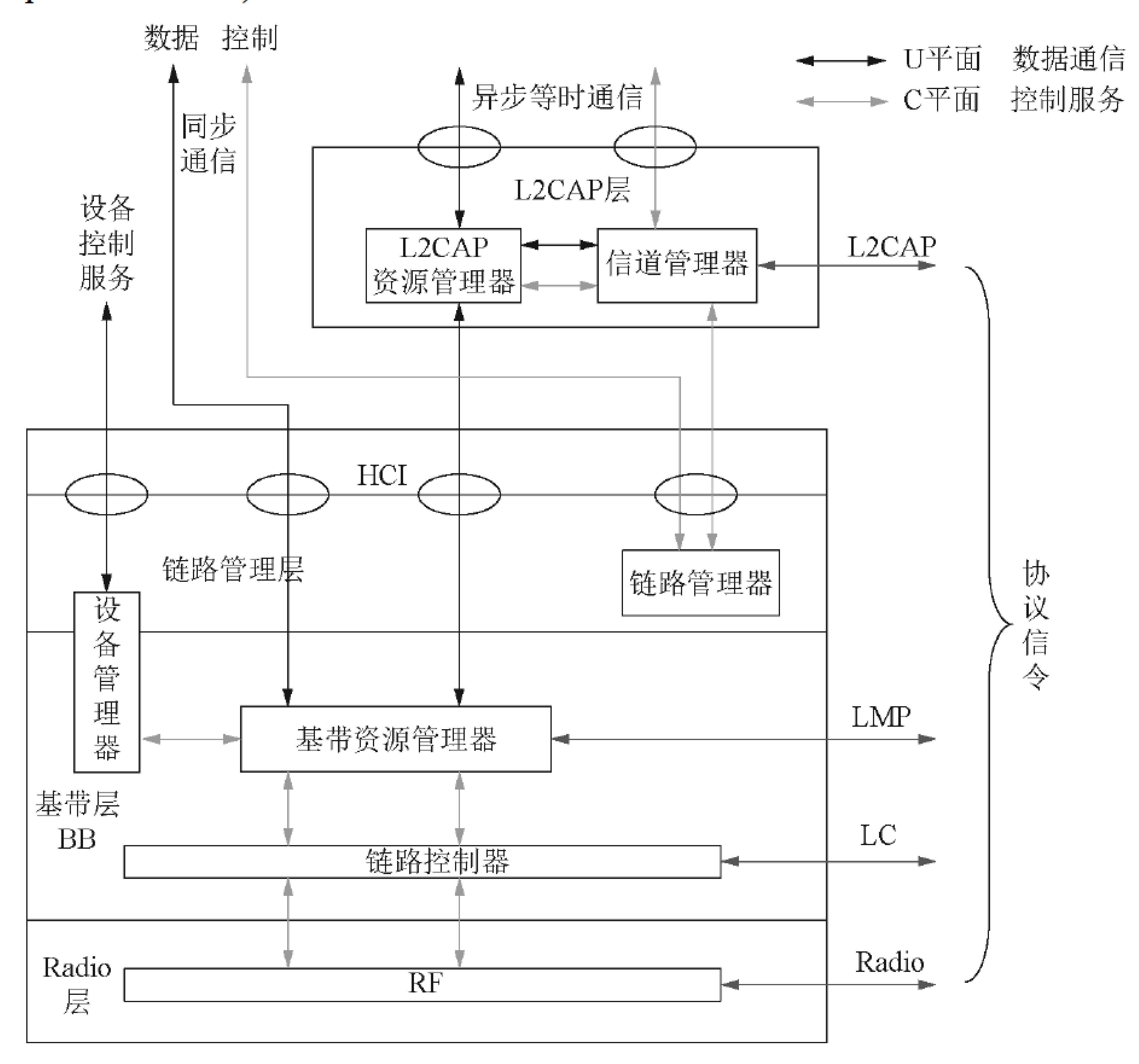


图 4.8 蓝牙核心系统体系结构

一条物理链路可以支持多条逻辑链路，只有逻辑链路才可以进行单播同步通信、异步等时通信或者广播通信，不同的逻辑链路用于支持不同的应用需求。

基带层和物理层的控制协议叫作链路管理协议(Link Manager Protocol，LMP)，用于控制设备的运行，并提供底层设施(PHY 和 BB)的管理服务。

逻辑链路控制和自适应协议 L2CAP 是对应用和服务的抽象，其功能是对应用数据进行分段和重装配，并实现逻辑链路的复用。

设备之间的互操作通过核心系统协议实现，主要的协议有 RF (Radio Frequency)协议、链路控制协议(Link Control Protocol，LCP)、链路管理协议 LMP 和 L2CAP 协议。

蓝牙控制器与高层之间的接口叫作主机控制器接口(Host Controller Interface，HCI)。

2. 核心功能模块

(1) 信道管理器：负责生成、管理和释放用于传输应用数据流的 L2CAP 信道。

(2) L2CAP 资源管理器：把 L2CAP 协议数据单元分段，并按照一定的顺序提交给基带层，而且还要进行信道调度，以保证一定 QoS 的 L2CAP 信道不会被物理信道(由于资源耗尽)所拒绝。

(3) 设备管理器：负责控制设备的一般行为。

(4) 链路管理器(LM)：负责生成、修改和释放逻辑链路及其相关的逻辑传输，并修改设备之间的物理链路参数。

(5) 基带资源管理器：负责对物理层的访问。它有两个主要功能，其一是调度功能，其二是与这些实体协商包含 QoS 承诺的访问合同。

(6) 链路控制器：负责根据数据负载和物理信道、逻辑传输和逻辑链路的参数对分组进行编码和译码。

(7) RF (Radio Frequency)：用于发送和接收物理信道上的数据分组。

3. 数据传输结构

L2CAP 服务对于异步的和等时的用户数据提供面向帧的传输。面向连接的 L2CAP 信道用于传输点对点单播数据。无连接的 L2CAP 信道用于广播数据。

L2CAP 信道的 QoS 设置定义了帧传送的限制条件，非帧的流式数据使用 SCO 逻辑传输。

核心系统支持通过 SCO (SCO-S)或扩展的 SCO (eSCO-S)直接传输等时的和固定速率的应用数据。应用从 BB 层选择最适当的逻辑链路类型来传输它的数据流。RF 信道通常是不可靠的，因此 BB 分组头使用了纠错编码，并且配合头校验和来发现残余差错。在 ACL 逻辑传输中实现了 ARQ 协议，通过自动请求重发来纠正错误。

4.2.3.2　ZigBee 技术

ZigBee 是基于 IEEE 802.15.4 开发的一组关于组网、安全和应用软件的技术标准。

1. IEEE 802.15.4 标准

802.15.4 定义的低速无线个人网(Low Rate-WPAN)包含两类设备，即全功能设备(FFD)和简单功能设备(RFD)。FFD 有 3 种工作模式，可以作为一般的设备、协调器或 PAN 协调器。FFD 可以与 RFD 或其他 FFD 通信，而 RFD 只能与 FFD 通信，RFD 之间不能互相通信。

LR-WPAN 网络的拓扑结构有星型网络和点对点网络两种。在星型拓扑中，只有在设备和 PAN 协调器之间才能通信，在设备之间不能互相通信。点对点网络与星型网络不同，这种网络中的所有设备之间都可以互相通信，只要处于信号覆盖范围之内。

802.15.4 定义的 LR-WPAN 体系结构如图 4.9 所示，物理层(PHY)包含 RF 收发器和底层管理功能，通过物理层管理实体服务访问点(PLME-SAP)和物理数据服务访问点(PD-SAP)向上层提供服务。

802.15.4—2006 标准定义的 4 种物理层如下。

- 868/915 MHz：直接序列扩频(DSSS)，二进制相移键控(BPSK)调制，数据速率为 20Kb/s 和 40Kb/s。
- 868/915 MHz：直接序列扩频(DSSS)，偏置正交相移键控(O-QPSK)调制，数据速率为 100Kb/s 和 250Kb/s。
- 868/915 MHz：并行序列扩频(PSSS)，二进制相移键控(BPSK)调制和幅度键控(ASK)调制，数据速率为 250Kb/s。
- 2.450 GHz：直接序列扩频(DSSS)，偏置正交相移键控(O-QPSK)调制，数据速率为 250Kb/s。

MAC 子层提供两种信道访问方式，即基于竞争的访问和无竞争的访问。基于竞争的访问方式应用了 CSIVIA/CA 后退算法，而且划分为不分时槽的和分时槽的两个不同版本。不

分时槽的 CSMA/CA 协议应用在未启用令牌的网络中，在启用令牌的网络中必须使用 CSMA/CA 协议的分时槽版本。

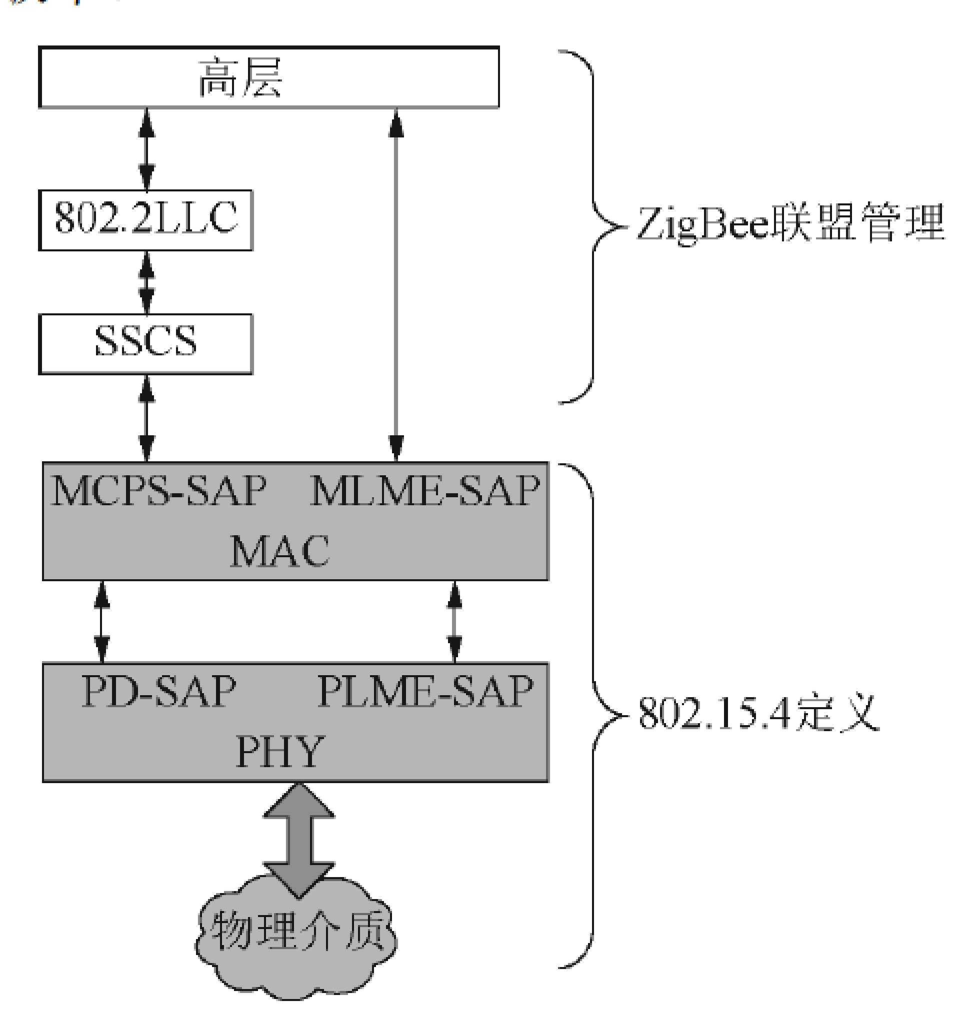


图 4.9 LR-WPAN 体系结构

2. ZigBee 网络

ZigBee 联盟主要任务如下。

(1) 定义 ZigBee 的网络层、安全层和应用层标准。

(2) 提供互操作性和一致性测试规范。

(3) 促进 ZigBee 品牌的全球化市场保证。

(4) 管理 ZigBee 技术的演变。

ZigBee 技术规范(2005)描述了 ZigBee 网络的基础结构和可利用的服务。ZigBee 网络层(NWK)提供了建立多跳网络的路由功能。APL 层包含了应用支持子层(APS)和 ZigBee 设备对象(ZDO)，以及各种可能的应用。ZDO 的作用是提供全面的设备管理，APS 的功能是对 ZDO 和各种应用提供服务。

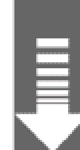
ZigBee 的安全机制分散在 MAC、NWK 和 APS 层，分别对 MAC 帧、NWK 帧和应用数据进行安全保护。ZigBee 的网络层和 MAC 层都使用高级加密标准 AES，以及结合了加密和认证功能的 CCM*分组加密算法。

ZigBee 协调器管理网络的路由功能。ZigBee 采用的路由算法是按需分配的距离矢量协议 AODV。当 NWK 数据实体要发送数分组时，如果路由表中不存在有效的路由表项，则首先要进行路由发现，并对找到的各个路由计算通路费用。

4.2.4 无线城域网

无线城域网目前比较成熟的标准有两个，一个是 2004 年颁布的 802.16d，这个标准支持无线固定接入，也叫作固定 WiMAX；另一个是 2005 年颁布的 802.16e，它是在前一标准的基础上增加了对移动性的支持，所以也称为移动 WiMAX。

WiMAX 技术主要有两个应用领域，一个是作为蜂窝网络、Wi-Fi 热点和 Wi-Fi Mesh



的回程链路；另一个是作为最后一千米的无线宽带接入链路。

移动 WiMAX (802.16e)向下兼容 802.16d，在移动性方面定位的目标速率为车速，可以支持 120km/h 的移动速率。IEEE 802.16 的协议栈模型由物理层和 MAC 层组成，MAC 层又分成了 3 个子层，即面向服务的汇聚子层、公共部分子层和安全子层。

4.2.4.1　关键技术

802.16 系统采用两个工作频段，其中，10G～66GHz 频段的工作波长较短，只能进行视距传输，在这个频段可以采用单载波调制方式。在 2G～11GHz 频段可以进行非视距传输，但必须考虑多径衰减的影响，这时每个子载波的调制方式可以选用 B/SK、QPSK、16-QAM 或 64-QAM。

802.16 采用的多路复用方式 OFDM/OFDMA 被认为是下一代无线通信网的关键技术。正交频分多址 OFDMA 是利用 OFDM 的概念实现上行多址接入。OFDMA 的引入是为了支持移动性。为了进一步提高带宽利用率，802.16 还引入了多入多出技术 MIMO。

802.16 系统以频分双工(FDD)或时分双工(TDD)方式工作。FDD 需要成对的频率，TDD 则不需要。

4.2.4.2　MAC 子层

802.16 MAC 层提供面向连接的服务。MAC 层定义了两种 CS 子层，即 ATM CS 和分组 CS，前者提供对 ATM 的业务支持，后者提供对 IEEE 802.3、IEEE 802.1q、IPv4 和 IPv6 等基于分组的业务的映射。

802.16 MAC 层定义了完整的 QoS 机制。为了更好地控制带宽分配，MAC 层定义了 4 种不同的业务。

- 非请求的带宽分配业务(UGS)：用于传输周期性的、包大小固定的实时数据，其典型的应用是 VoIP 电话。
- 实时轮询业务(rtPS)：用于支持周期性的、包大小可变的实时业务，例如 MPEG 视频业务。
- 非实时轮询业务(nrtPS)：用于支持非实时可变速率业务，例如高带宽的 FTP 应用。
- 尽力而为业务(BE)：用于支持非实时性、无任何速率和时延要求的分组业务，典型业务是 Telnet 和 HTTP 服务。

4.2.4.3　向 4G 迈进

1. 802.16e

802.16d 的 OFDM 调制方式采用 256 个子载波，OFDMA 调制方式采用 2048 个子载波，信号带宽在 1.25M～20MHz 可变。为了支持移动性，802.16e 对物理层进行了改进，使得 OFDMA 可支持 128、512、1024 和 2048 共 4 种不同的子载波数量，但子载波间隔不变，信号带宽与子载波数量成正比，这种技术被称为可扩展的 OFDMA(Scalable OFDMA)。采用这种技术，系统可以在移动环境中灵活地适应信道带宽的变化。在采用 20MHz 带宽、64-QAM 调制的情况下，传输速率可达到 74.81Mbps。

2. WiMAX II

ITU-R 对 4G 标准的要求是能够提供基于 IP 的高速声音、数据和流式多媒体服务，支持的数据速率至少是 100Mb/s，选定的通信技术是正交频分多址接入技术 OFDMA。

最初候选的 4G 标准有 3 个，即 UMB(Ultra Mobile Broadband)、LTE(Long Term Evolution)和 WiMAX II(IEEE 802.16m)。

UMB 的最高下载速率可达到 288Mb/s，最高上传速率可达到 75Mb/s，支持的终端移动速率超过 300km/h。2008 年 11 月，高通公司宣布放弃 UMB 技术。

LTE(Long Term Evolution)采用 OFDM/OFDMA 作为物理层的核心技术，支持 1.25M～20MHz 宽带，峰值速率下行 1Gb/s，上行 500Mb/s。

IEEE 802.16m 支持 5M～20MHz 的抗辩带宽，特殊情况下可达 100MHz，其下行峰值速率在低速移动、热点覆盖条件下可以达到 1Gb/s，在高速移动、广域覆盖条件下可以达到 100Mb/s。

2013 年年底，中华人民共和国工业和信息化部正式向三大电信运营商发放了 4G 牌照，中国移动、中国电信和中国联通均获得 TD-LTE 牌照。

(1) 中国移动：1880M～1900MHz、2320M～2370MHz、2575M～2635MHz。

(2) 中国联通：2300M～2320MHz、2555M～2575MHz。

(3) 中国电信：2370M～2390MHz、2635M～2655MHz。

4.3 真题详解

试题 1 (2017 年下半年试题 44)

无线局域网通常采用的加密方式是 WPA2，其安全加密算法是__(44)__。

(44) A. AES 和 TKIP　　B. DES 和 TKIP

C. AES 和 RSA　　D. DES 和 RSA

参考答案：(44) A。

要点解析：WPA2 避免了 WEP 的相关问题，它使用 AES 加密数据，并定义了一个具有更高安全性的加密标准 CCMP，密码使用 TKIP 方式。

试题 2 (2017 年下半年试题 57)

采用 CSMA/CD 协议的基带总线，段长为 1000M，数据速率为 10Mb/s，信号传播速度为 200m/μs，则该网络上的最小帧长应为__(57)__比特。

(57) A.50　　B.100　　C.150　　D.200

参考答案：(57) B。

要点解析：发送时间应大于等于两倍的端到端的传播时间。单程需要的传播时间为 1000/200=5μs，两倍的端到端传播时间也就是往返时间为 10μs。数据速率为 10Mb/s，则最小帧长为 10Mb/s×10μs=100bit。



试题 3 （2017 年上半年试题 34）

在以太网中发生冲突时采用退避机制，__(34)__优先传输数据。

(34) A. 冲突次数最少的设备　　B. 冲突中 IP 地址最小的设备
C. 冲突域中重传计时器首先过期的设备　D. 同时开始传输的设备

参考答案：(34) C。

要点解析：退避机制规定，在发生冲突时，由冲突域中重传计时器首先过期的设备优先传输数据。

试题 4 （2017 年上半年试题 64）

在以太网中出于对__(64)__的考虑，需设置数据帧的最小帧。

(64)A. 重传策略　B. 故障检测　C. 冲突检测　D. 提高速率

参考答案：(64)C。

要点解析：为了确保发送数据站点在传输时能检测到可能发生的冲突，数据帧的传输时延要不小于两倍的传播时延。

试题 5 （2017 年上半年试题 66）

802.11g 标准的最高数据传输速率为__(66)__Mb/s。

(66)A. 11　B. 28　C. 54　D. 108

参考答案：(66)C。

要点解析：802.11g 标准运行频段为 2.4GHz 的 ISM 频段，使用的主要技术是 ODDM 调制技术，其数据速率为 54Mb/s。

试题 6 （2016 年下半年试题 65）

IEEE 802.11 标准采用的工作频段是__(65)__。

(65) A. 900MHz 和 800MHz　B. 900MHz 和 2.4GHz
C. 5GHz 和 800MHz　D. 2.4GHz 和 5GHz

参考答案：(65)D。

要点解析：IEEE 802.11 标准采用的工作频段是 2.4GHz 和 5GHz。

试题 7 （2016 年下半年试题 66）

IEEE 802.11 MAC 子层定义的竞争性访问控制协议是__(66)__。

(66) A. CSMA/CA　B. CSMA/CB　C. CSMA/CD　D. CSMA/CG

参考答案：(66)A。

要点解析：CSMA/CD 虽然已经成功应用于适用有线连接的局域网，但在无线局域网的环境下不能简单地搬用，特别是冲突检测部分，IEEE 802.11 MAC 子层定义的竞争性访问控制协议是 CSMA/CA。

试题 8 （2016 年下半年试题 67）

无线局域网的新标准 IEEE 802.11n 提供的最高数据速率可达到__(67)__Mb/s。

(67) A. 54　B. 100　C. 200　D. 300

参考答案：(67)D。

要点解析：802.11n 可工作在 2.4GHz 和 5GHz 两个频段，速率可达到 300Mb/s，使用 MIMO 技术可以达到 600Mb/s。

试题 9 (2016 年上半年试题 65 和试题 66)

IEEE 802.11MAC 子层定义的竞争性访问控制协议是__(65)__。之所以不采用与 IEEE 802. 3 相同协议的原因是__(66)__。

(65) A. CSMA/CA　B. CSMA/CB　C. CSMA/CD　D. CSMA/CG

(66) A. IEEE 802.11 协议的效率更高　B. 为了解决隐蔽终端问题

C. IEEE 802.3 协议的开销更大　D. 为了引进多种非竞争业务

参考答案：(65)A；(66)B。

要点解析：CSMA/CD 协议虽然已经成功运用于用有线连接的局域网，但在无线局域网的环境下，不能简单搬用 CSMA/CD 协议，特别是冲突检测部分。主要原因有两个。

① 在无线局域网中，接收信号的强度往往会远小于发送信号的强度，因此如果要实现冲突检测的话，在硬件上的花费就会比较大。

② 在无线局域网中，并非所有的站点都能监听到对方，而“所有站点都能监听到对方”正是 CSMA/CD 协议的基础。

CSMA/CD：带有冲突检测的载波监听多路访问，可以检测冲突，但无法“避免”。

CSMIA/CA：带有冲突避免的载波监听多路访问，发送包的同时不能检测到信道上有无冲突，只能尽量“避免”。

试题 10 (2015 年下半年试题 62)

以下关于 CSMA/CD 协议的叙述中，正确的是__(62)__。

(62) A. 每个节点按照逻辑顺序占用一个时间片轮流发送

B. 每个节点检查介质是否空闲，如果空闲则立即发送

C. 每个节点想发就发，如果没有冲突则继续发送

D. 得到令牌的节点发送，没有得到令牌的节点等待

参考答案：(62) B。

要点解析：每个以太网节点利用总线发送数据时，首先需要侦听总线是否空闲。以太网的物理层规定发送的数据采用曼彻斯特编码方式。如果总线上已经没有数据在传输，总线的电平将不会发生跳变，可以判断此时为“总线空闲”。如果一个节点已准备好发送的数据帧，并且总线此时处于空闲状态，则这个节点就可以“启动发送”。

试题 11 (2015 年下半年试题 64 和试题 65)

ITU-R 对 4G 标准的要求是能够提供基于 IP 的高速语音、数据和流式多媒体服务，支持的数据速率至少是__(64)__，选定的多路复用技术是__(65)__。

(64) A. 10Mb/s　B. 100Mb/s　C. 20Mb/s　D. 1Gb/s

(65) A. OFDM　B. QPSK　C. MIMO　D. 64-QAM

参考答案：(64) B；(65) A。

要点解析：ITU-R 对 4G 标准的要求是能够提供基于 IP 的高速语音、数据和流式多媒体服务，支持的数据速率至少是 100Mb/s，选定的复用技术是(正交频分复用)。这是一种无



线环境下的高速传输技术，其主要思想就是在频段内将给定信道分成许多正交子信道，在每个子信道上使用一个子载波进行调制，各子载波并行传输。OFDM 技术的优点是可以消除或减小信号波形间的干扰，对多径衰落和多普勒频移不敏感，提高了频谱利用率。

试题 12　(2015 年上半年试题 49)

IEEE 802.1x 是一种基于 (49) 的认证协议。

(49) A. 用户 ID　　B. 报文　　C. MAC 地址　　D. SSID

参考答案：(49) C。

要点解析：IEEE 802.1x 是一种基于端口的网络接入控制技术，在 LAN 设备的物理接入级对接入设备进行认证和控制，此处的物理接入级指的是 LANSWITCH 设备的端口。它可以限制未经授权的用户/设备通过接入端口(access port)访问 LAN/WLAN。在获得交换机或 LAN 提供的各种业务之前，802.1x 对连接到交换机端口上的用户/设备 MAC 地址进行认证。

试题 13　(2015 年上半年试题 50)

为了弥补 WEP 协议的安全缺陷，WPA 安全认证方案增加的机制是 (50) 。

(50) A. 共享密钥认证　　B. 临时密钥完整性协议
C. 较短的初始化向量　　D. 采用更强的加密算法

参考答案：(50) B。

要点解析：在 WPA 的设计中包含了认证、加密和数据完整性校验 3 个组成部分。首先是 WPA 使用了 802.1x 协议对用户的 MAC 地址进行认证；其次是 WEP 增大了密钥和初始向量的长度；WPA 还采用了可以动态改变密钥的临时密钥完整性协议 TKIP。最后，WPA 强化了数据完整性保护。

试题 14　(2015 年上半年试题 62)

4G 移动通信标准 TD-LTE 与 FDD-LTE 的区别是 (62) 。

(62) A. 频率的利用方式不同　　B. 划分上下行信道的方式不同
C. 采用的调制方式有区别　　D. 拥有专利技术的厂家不同

参考答案：(62) A。

要点解析：TD-LTE 与 FDD-LTE 的区别不大，都属于 LTE 的分支。FDD(Frequency Division Duplexing)是频分双工，有两个独立的信道，一个用来向下传送信息，另一个用来向上传送信息。两个信道之间存在一个保护频段，以防止邻近的发射机和接收机之间产生相互干扰。而 TDD (Time Division Duplexing)是时分双工，发射和接收信号是在同一频率信道的不同时隙中进行的，彼此之间采用一定的保证时间予以分离。

试题 15　(2015 年上半年试题 63)

关于移动 Ad Hoc 网络 MANET， (63) 不是 MANET 的特点。

(63) A. 网络拓扑结构是动态变化的
B. 电源能量限制了无线终端必须以最节能的方式工作
C. 可以直接应用传统的路由协议支持最佳路由选择
D. 每个节点既是主机又是路由器

参考答案：(63) C。

要点解析：移动 Ad Hoc 网络(MANET)是一种与传统有基站无线网络相对的无中心结构通信网，也被称为自组网。但无线网络的动态结构特点，以及无线终端的电源能量有限，使传统的路由协议不能直接应用于 MANET。目前已经提出了多种 MANET 路由协议，如目标排序的距离矢量协议 DSDV、按需分配的距离矢量协议 AODV 等。

4.4 强化训练

4.4.1 综合知识试题

试题 1 (2014 年下半年试题 47)

在无线局域网中，AP(无线接入点)工作在 OSI 模型的__(47)__。

(47) A. 物理层　　B. 数据链路层　　C. 网络层　　D. 应用层

试题 2 (2014 年下半年试题 62)

以太网采用 CSMA/CD 协议，当冲突发生时要通过二进制指数后退算法计算后退时延，关于这个算法，以下论述中错误的是__(62)__。

(62) A. 冲突次数越多，后退的时间越短
B. 平均后退次数的多少与负载大小有关
C. 后退时延的平均值与负载大小有关
D. 重发次数达到一定极限后放弃发送

试题 3 (2014 年下半年试题 64)

以下通信技术中，未在 IEEE 802.11 无线局域网中使用的是__(64)__。

(64) A. FHSS　　B. DSSS　　C. CDMA　　D. IR

试题 4 (2014 年下半年试题 65)

ZigBee 网络是 IEEE 802.15.4 定义的低速无线个人网，其中包含全功能和简单功能两类设备，以下关于这两类设备的描述中，错误的是__(65)__。

(65) A. 协调器是一种全功能设备，只能作为 PAN 的控制器使用
B. 被动式红外传感器是一种简单功能设备，接受协调器的控制
C. 协调器也可以运行某些应用，发起和接受其他设备的通信请求
D. 简单功能设备之间不能互相通信，只能与协调器通信

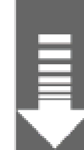
试题 5 (2014 年上半年试题 60)

中国自主研发的 3G 通信标准是__(60)__。

(60) A. CDMA 2000　　B. TD-SCDMA　　C. WCDMA　　D. WiMAX

试题 6 (2014 年上半年试题 61)

IEEE 802.11 规定了多种 WLAN 的通信标准，其中__(61)__与其他标准采用频段不



同，因而不能兼容。

(61) A.IEEE 802.11a　　B. IEEE 802.11b
C. IEEE 802.11g　　D. IEEE 802.11n

试题 7　(2014 年上半年试题 62 和试题 63)

IEEE 802.11 定义的 Ad Hoc 网络是由无线移动节点组成的对等网，这种网络的特点是__(62)__。在这种网络中使用的 DSDV(Destination-Sequenced Distance Vector)路由协议是一种__(63)__。

(62) A. 每个节点既是主机，又是交换机
B. 每个节点既是主机，又是路由器
C. 每个节点必须通过中心节点才能互相通信
D. 每个节点都发送 IP 广播包来与其他节点通信

(63) A. 洪泛式路由协议　　B. 随机式路由协议
C. 链路状态路由协议　　D. 距离矢量路由协议

4.4.2　综合知识试题参考答案

【试题 1】答　案：(47)B。

解　析：OSI 是 Open System Interconnect 的缩写，意为开放式系统互连。一般称作 OSI 参考模型。该体系结构标准定义了网络互连的七层框架(物理层、数据链路层、网络层、传输层、会话层、表示层和应用层)。

在基础设施网络中，无线终端通过接入点(Access Point，AP)访问骨干网上的设备，或者互相访问。接入点如同一个网桥，它负责在 802.11 和 802.3 MAC 协议之间进行转换。无线局域网的协议结构如图 4.10 所示。

<table>
<tr><td rowspan="2">数据链路层</td><td>LLC</td><td></td><td rowspan="4">站
管
理</td></tr>
<tr><td>MAC</td><td>MAC 管理</td></tr>
<tr><td rowspan="2">物理层 PHY</td><td>PLCP</td><td rowspan="2">PHY 管理</td></tr>
<tr><td>PMD</td></tr>
</table>

图 4.10　无线局域网的协议结构图

【试题 2】答　案：(62)A。

解　析：按照二进制指数后退算法，后退时延的取值范围与重发次数 n 形成二进制指数关系。随着重发次数 n 的增加，后退时延的取值范围按 2 的指数增大。

【试题 3】答　案：(64)C。

解　析：码分多址(CDMA)是在数字技术的分支——扩频通信技术上发展起来的一种崭新而成熟的移动通信技术。CDMA 技术的标准化经历了几个阶段。IS-95 是 CDMA ONE 系列标准中最先发布的标准，真正在全球得到广泛应用的第一个 CDMA 标准是 IS-95A。

FHSS 跳频技术 (Frequency-Hopping Spread Spectrum)、DSSS 直接序列展频技术(Direct Sequence Spread Spectrum)、IR 红外线(Infrared Radiation)，都属于 WLAN 通信技术，在 IEEE 802.11 无线局域网中使用。

【试题 4】答　案：(65)A。

解　析：ZigBee 网络中包含全功能(FFD)和简单功能(RFD)两类设备，在一个 ZigBee 网络中，至少存在一个 FFD 充当整个网络的协调器，即 PAN 协调器，ZigBee 中也称作 ZigBee 协调器。一个 ZigBee 网络只有一个 PAN 协调器。通常，PAN 协调器是一个特殊的 FFD，它具有较强大的功能，是整个网络的主要控制者，它负责建立新的网络、发送网络信标、管理网络中的节点以及存储网络信息等。FFD 和 RFD 都可以作为终端节点加入网络。

【试题 5】答　案：(60) B。

解　析：中国移动的 3G 网络采用的是中国自主创新的 TD-SCDMA 技术，业务品牌为“G3”。

【试题 6】答　案：(61)A。

解　析：IEEE 802.11 先后提出了以下多个标准，最早的 802.11 标准只能够达到 1M～2Mb/s 的速度，在制定更高速度的标准时，就产生了 802.11a 和 802.11b 两个分支，后来又推出了 802.11g 的新标准。

- IEEE 802.11，1997 年推出，速率为 1Mb/s 和 2Mb/s，工作在 2.4GHz 频段。
- IEEE 802.11a，1999 年推出，速率为 54Mb/s，工作在 5GHz 频段。
- IEEE 802.11b，1999 年推出，速率为 11Mb/s，工作在 2.4GHz 频段。
- IEEE 802.11g，2003 年推出，速率为 54Mb/s，工作在 2.4GHz 频段。
- IEEE 802.11n，2009 年 9 月通过正式标准，WLAN 的传输速率由 802.11a 及 802.11g 提供的 54Mb/s、108Mb/s，提高到 350Mb/s，甚至高达 475Mb/s，工作在 2.4GHz 和 5GHz 频段。

【试题 7】答　案：(62)B；(63)D。

解　析：Ad Hoc(点对点)模式：Ad Hoc 模式就和以前的直连双绞线概念一样，是 P2P 的连接，所以也就无法与其他网络沟通了。一般无线终端设备像 PMP、PSP、DMA 等用的就是 Ad Hoc 模式。

Ad Hoc 结构是一种省去了无线中介设备 AP 而搭建起来的对等网络结构，只要安装了无线网卡，计算机彼此之间即可实现无线互连。其原理是网络中的一台计算机主机建立点到点连接，相当于虚拟 AP，而其他计算机就可以直接通过这个点对点连接进行网络互连与共享。

Destination-Sequenced Distance-Vector(DSDV)是一种适用于 Ad Hoc 网络的表驱动式路由协议。此协议以 Bellman-Ford 算法为基础，在 RIP 的基础上设计完成。此算法在 1994 年由 C. Perkins 和 P. Bhagwat 提出。DSDV 协议通过给每个路由设定序列号避免了路由环路的产生，每个节点保存一份路由表，表中的每一条记录都有一个序列号，偶数序列号表示此 link 存在，由目的地址对应的节点生成，奇数序列号表示 link 已经破损，由发现 link 破损的节点生成。其中 Bellman-Ford 算法就是距离矢量路由协议算法。

第 5 章 网络互连与互联网

5.1 备考指南

5.1.1 考纲要求

根据考试大纲中相应的考核要求，在“网络互连与互联网”知识模块上，要求考生掌握以下方面的内容。

(1) 常见的网络互连设备：中继器、Hub、网桥、交换机、路由器、网关的工作原理，以及与 OSI 的七层模型关系，广播域和冲突域。

(2) IP 协议：IP 地址、IP 协议的操作、IP 协议数据单元。

(3) ICMP 协议。

(4) TCP 与 UDP 协议：TCP 服务、TCP 协议、TCP 拥塞控制、UDP 协议。

(5) 域名与地址：域名系统、地址分解协议。

(6) 网关协议：自治系统、外部网关协议、内部网关协议、核心网关协议。

(7) 路由器技术：NAT 技术、CIDR 技术、第三层交换技术。

(8) IP 组播技术：组播模型概述、组播地址、因特网组管理协议和组播路由协议。

(9) IP QoS 技术：集成服务、区分服务、流量工程。

(10) Internet 应用：远程登录协议、文件传输协议、简单邮件传输协议、超文本传输协议和 P2P 应用。

5.1.2 考点统计

“网络互连与互联网”知识模块在历次网络工程师考试试卷中出现的考核知识点及分值分布情况如表 5.1 所示。

表 5.1　历年考点统计表

年　份	题　号	知识点	分值
2017 年下半年	上午：19～25、27～29、38～41、48～55、60	OSPF 协议、TCP 协议、IP 数据报格式、RSVP 协议、BGP 协议、ARP 协议、电子邮件、HTTPS 协议、子网划分和子网掩码、CIDR 和路由汇聚、IP 组播技术、ICMP	23 分
	下午：无	无	0 分
2017 年上半年	上午：20～30、51～55	IPv4、TCP 协议、RIP 协议、ARP 协议、OSPF 协议、子网划分和子网掩码	16 分
	下午：无	无	0 分
2016 年下半年	上午：13、20～27、34～38、51～55	TCP/IP 协议、UDP 协议，ARP、RIP、OSPF 协议，电子邮件协议，子网划分和子网掩码，CIDR 和路由汇聚，DNS 协议	19 分
	下午：无	无	0 分
2016 年上半年	上午：20～34、37～40、51～55	IP 组播技术、IP QoS、RIP 路由协议、OSPF 协议、DNS 协议、CIDR 和路由汇聚、电子邮件协议	24 分
	下午：无	无	0 分
2015 年下半年	上午：11、14、20～22、24～29、35～38、51～56、67	集线器和网桥、ICMP 协议、TCP 协议、边界网关协议 BGP4、OSPF 协议、电子邮件协议、CIDR 和路由汇聚、子网划分和子网掩码、MPLS	22 分
	下午：无	无	0 分
2015 年上半年	上午：13、16～19、21、26、28、51、52、59、61、65	网桥、路由器技术、OSPF 协议、RIP 路由协议、VoIP 网络电话、子网划分和子网掩码、地址解析协议	13 分
	下午：无	无	0 分
2014 年下半年	上午：22～25、53～56、61	边界网关协议 BGP4、IGRP 协议、RIP 协议、自动专用 IP 地址、IP 地址划分、主机地址、IP 地址汇聚、TCP 连接的建立	9 分
	下午：无	无	0 分
2014 年上半年	上午：16～22、30、51～55、64～69	组播地址区、区分服务、ICMP 协议、RIP 路由协议、HTTP1.1、IP 地址配置、VLSM 编址、单播地址、OSPF 协议、NAT 技术、CIDR 技术	15 分
	下午：无	无	0 分
2013 年下半年	上午：16～18、21、22、29、30、36、37、51～55，60～65	TCP 和 UDP 报头、RSVP 协议、IP 和 TCP 数据报、TCP 报文、SMTP 协议、POP3 协议、CIDR 地址、路由汇聚、子网划分、子网掩码、链路聚合、TCP 协议	6 分
	下午：无	无	0 分
2013 年上半年	上午：11，13、14、18，21～27，40，52、53，55、56，58，69	路由器的功能、ICMP 报文、ARP 地址解析、分层编址、链路状态路由协议、网桥和交换机、路由器的特点、OSPF 区域划分、RIPV2 路由协议、子网划分、电子邮件协议、子网掩码、路由汇聚、CIDR 地址、公网 IP 地址	4 分
	下午：无	无	0 分

年　份	题　号	知 识 点	分 值
2012 年下半年	11、12、18～27、39、40、49、52～58、60、61	广播地址、D 类地址、自动专用 IP 地址、子网划分、主机地址、ICMP 协议、SNMP Trap、TCP 与 UDP、TCP 连接状态、RARP 协议、代理 ARP、距离矢量路由协议、BGP4 协议、链路状态算法、路由协议、地址伪装、路由汇聚、地址分配、匿名访问、电子邮件协议	6 分
	下午：无	无	0 分
2012 年上半年	上午：12、18～27、31、52～58、60	冲突域与广播域、私网地址、子网划分、主机地址与广播地址、C 类地址、子网掩码、主机地址、ICMP 协议、TCP 连接建立与释放、ARP 协议、RIP 协议、OSPF 协议、SMTP 传输的邮件报文格式、FTP 默认的控制连接端口	10 分
	下午：无	无	0 分

5.1.3　命题特点

本章内容是上午考试的重点。

纵观历年试卷，本章知识点是以选择题的形式出现在试卷中的。本章知识点在历次考试上午试卷中，所考查的题量为 10～17 道选择题，所占分值为 10～17 分(占试卷总分值 75 分中的 13%～23%)。本章试题偏重于理论，检验考生是否理解相关的知识点，考试难度中等。IP 地址、子网划分、路由协议、路由汇聚、TCP 协议是本章考核的重点内容，要掌握好。

5.2　考点串讲

5.2.1　网络互连设备

网络互连设备的作用是连接不同的网络，它们根据工作的协议层进行分类：中继器工作于物理层；网桥和交换机工作于数据链路层；路由器工作于网络层；网关则工作于网络层以上的协议层。

5.2.1.1　中继器和集线器

1. 中继器

中继器(Repeater)工作在 OSI 模型的物理层，其主要功能是对接收信号进行再生和发送。中继器不解释也不改变接收到的数字信息，它只从接收信号中分离出数字数据，存储起来，然后重新构造它并转发出去。再生的信号与接收信号完全相同，并可以沿着另外的网段传输到远端。

以太网中对中继器的使用上限控制在 4 个，即最多由 5 个网段组成。而且中继器也不能把传输介质不同的网络连接在一起。

2. 集线器

集线器(Hub)也工作在OSI模型的物理层，其工作原理与中继器基本相同。简单地说，集线器就是一个多端口的中继器，可作为网络传输介质间的中央节点。集线器分为无源(Passive)集线器、有源(Active)集线器和智能(Intelligent)集线器。无源集线器只负责把多段介质连接在一起，不对信号作任何处理，每一种介质段只允许扩展到最大有效距离的一半。

5.2.1.2 网桥

网桥(Bridge)是一种连接局域网的网络互连设备，工作在数据链路层。网桥具有过滤帧的功能，通过分析帧地址字段，来决定是否把收到的帧转发到另一个网络段上。

当网桥收到一个帧时，并不是向所有端口转发此帧，而是先检查此帧的源地址和目的地址。如果目的地址和源地址不在同一个网段上，它就把帧转发到另一个网段上；若两个地址在同一个网段上，则不转发。网桥的工作原理图如图5.1所示。

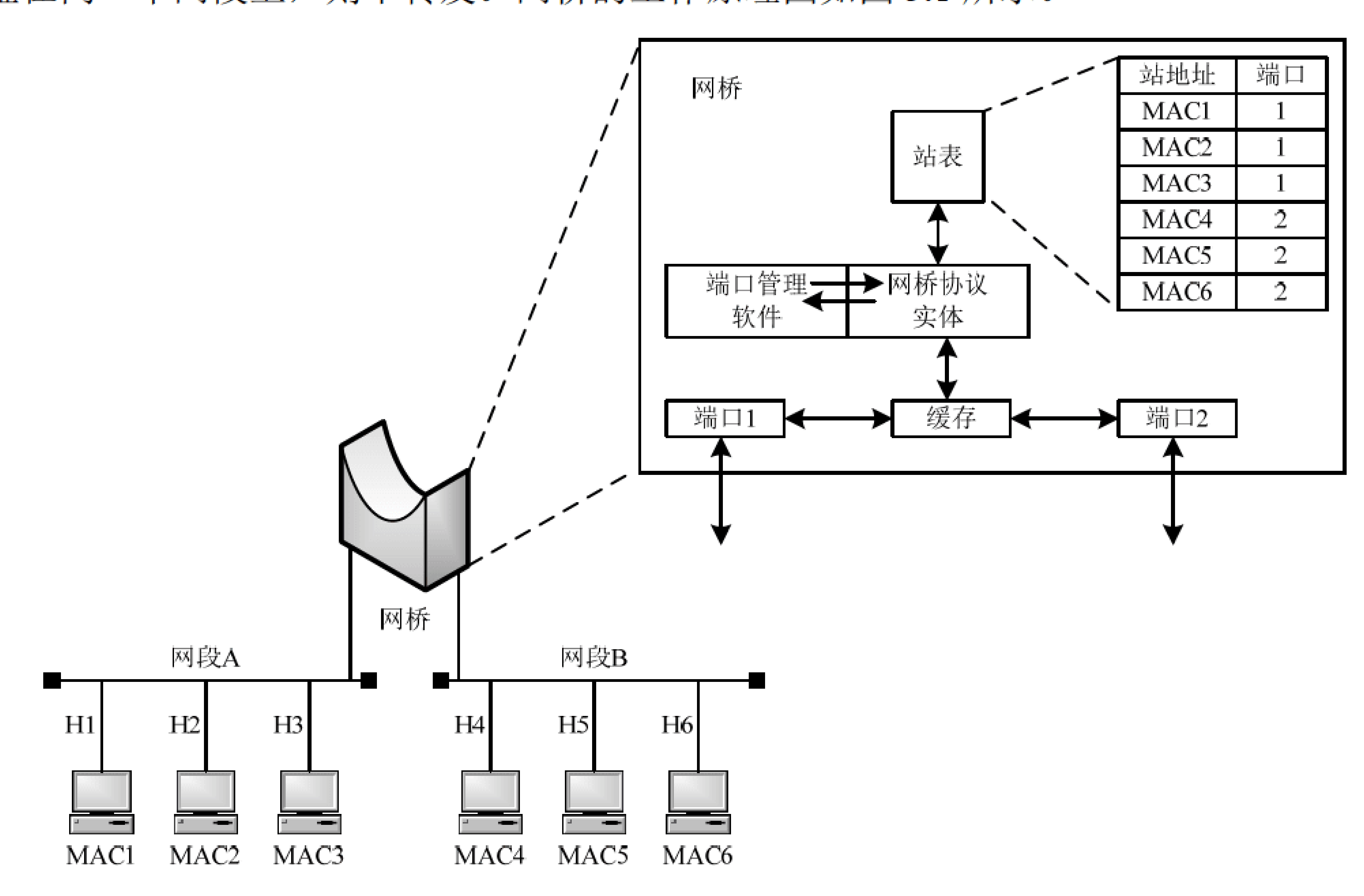
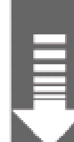


图5.1 网桥的工作原理

- 在图5.1中，若工作站H1向工作站H2发送以太网帧，因工作站H2与工作站H1在同一个物理网段上，网桥对此帧进行过滤，不转发该帧。
- 若工作站H1向工作站H4发送以太网帧，网桥通过查找网桥表知道工作站H4与网桥端口2对应，于是就将该帧从端口2转发。
- 若工作站H1向工作站H7发送以太网帧，而在网桥地址表中未找到关于工作站H7的MAC地址与端口的对应关系，此时，网桥会把这个发往未知目的MAC地址的帧向除发送该帧的源端口外的其他所有端口进行转发。在这种情况下，网桥实际上充当的是集线器的角色，确保没有使信息停止传送。

网桥工作在MAC子层，只要两个网络MAC子层以上的协议相同，都可以用网桥互连。另外，网桥还可以连接不同传输介质的网络。



以太网中广泛使用的交换机是一种多端口网桥，每个端口可以连接一个局域网。

5.2.1.3　路由器

路由器适合于连接复杂的大型网络，它工作在网络层，可以连接下面三层执行不同协议的网络，协议的转换由路由器完成，从而消除了网络层协议之间的差别。通过路由器连接的子网在网络层之上必须执行相同的协议。

相比于网桥，路由器的互连能力更强，可以执行复杂的路由选择算法。路由器处理的信息量比网桥要多，因此处理速度比网桥慢。要注意的是，路由桥是具有路由选择功能的网桥，路由桥虽然能运行路由选择算法，但它不涉及第三层协议，仍工作在数据链路层。

5.2.1.4　网关

网关是最复杂的网络互连设备，它用于连接网络层之上执行不同协议的子网，组成异构型的互联网。为了实现异构型设备之间的通信，网关要对不同的传输层、会话层、表示层和应用层协议进行翻译和变换。

由于其工作复杂，因而用网关因特网时效率比较低，而且透明性不好。因而网关往往用于针对某种特殊用途的专用连接。有时并不划分路由器和网关，而把网络层及其以上进行协议转换的互连设备统称为网关。

5.2.1.5　冲突域和广播域的概念

(1) 冲突域：是指连接在同一导线上的所有工作站的集合。这个域代表了冲突在其中发生并传播的区域，这个区域可以被认为是共享段。在 OSI 模型中，冲突域被看作是第一层的概念，连接同一冲突域的设备有集线器(Hub)、中继器(Repeater)或者其他进行简单复制信号的设备。也就是说，用 Hub 或者 Repeater 连接的所有节点可以被认为是在同一个冲突域内，它不会划分冲突域。而第二层设备(如网桥、交换机)和第三层设备(如路由器)都可以划分冲突域。

(2) 广播域：是指接收同样广播消息的节点的集合。由于广播域被认为是 OSI 中的第二层概念，所以像网桥、交换机等第二层设备连接的节点被认为都是在同一个广播域内。而路由器、第三层交换机则可以划分广播域。

5.2.2　广域网互连

广域网互连一般采用在网络层进行协议转换的方法实现。这里使用的互连设备叫作网关，更确切地说是路由器。

5.2.2.1　OSI 网络层内部结构

为了实现类型不同的子网互连，OSI 把网络层划分为 3 个子层：子网访问层、子网相关层和子网无关层。

- 子网访问层对应于实际网络的第三层，它不一定符合 OSI 的网络层标准。如果两个实际网络的子网访问子层不同，则它们不能简单地互连。
- 子网相关层的作用是增强实际网络的服务，使其接近于 OSI 的网络层服务，两个

不同类型的子网经过分别增强后可达到相同的服务水准。

- 子网无关层提供标准的 OSI 网络服务，它利用子网相关层提供的功能，按照 OSI 网络层协议实现两个子网的互连。

5.2.2.2 面向连接的网际互连

实现面向连接的网际互连的前提是子网提供面向连接的服务，这样可以用路由器连接两个或多个子网，路由器是每个子网的 DTE。当不同子网中的 DTE 要进行通信时，就通过路由器建立一条跨网络的虚电路。这种网际虚电路是通过路由器把两个子网中的虚电路级连起来实现的。如图 5.2 所示，主机 A 和主机 B 通过建立的虚电路传送信息。

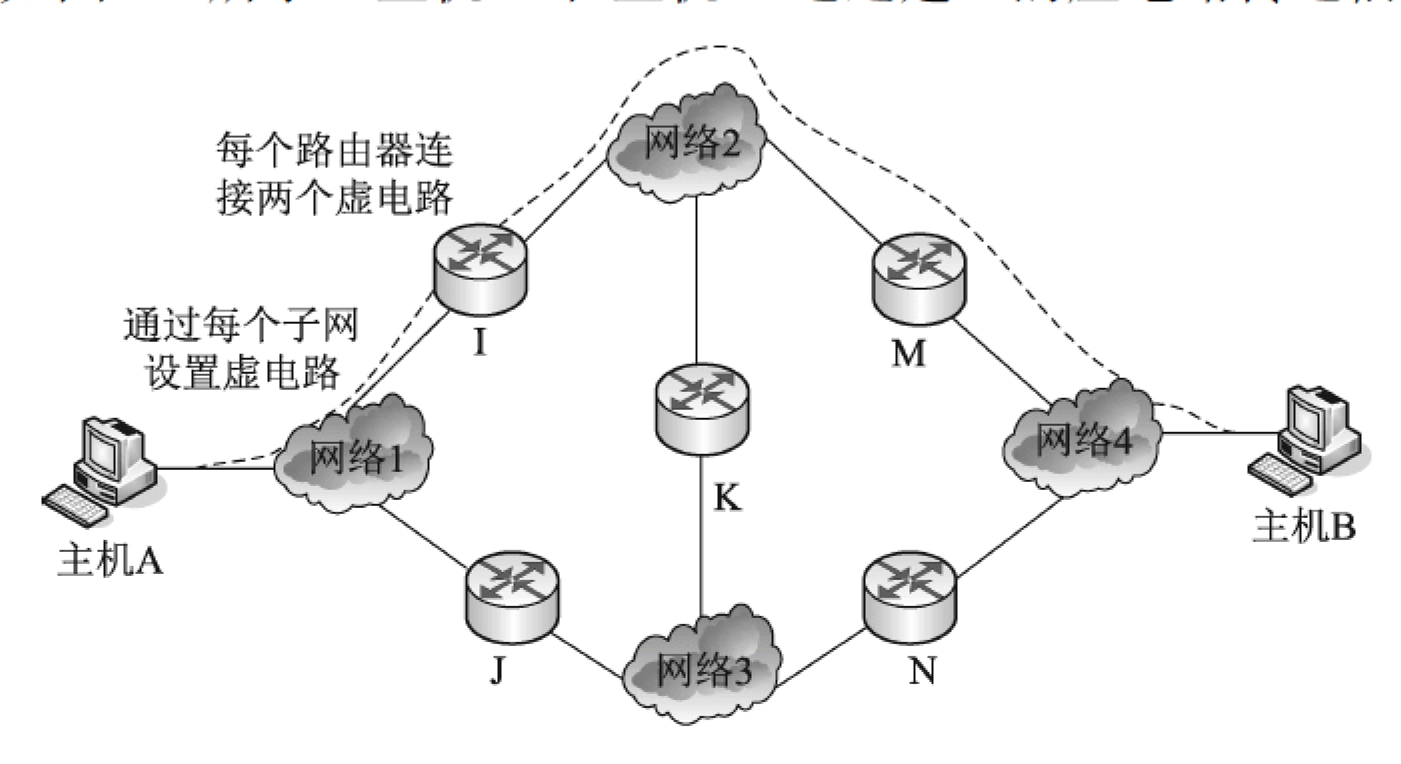


图 5.2　面向连接的解决方案

面向连接的解决方案要求互联网中的每一个物理网络都能提供面向连接的服务，但这样的要求在实际中是不现实的。

5.2.2.3 无连接的网际互连

如果网络仍采用图 5.2 的拓扑结构，在无连接的方案中，主机 A 和主机 B 之间通信时不要建立虚电路，数据单元在网络中分别独立传输，这些数据单元经过一系列的网络和路由器，最终到达目的节点。由于网络设备对每个数据单元的路由选择是独立进行的，因此不同的数据单元到达目的主机经过的路径可能不同。

目前，流行的互联网就是采用了面向无连接的解决方案。IP 协议是面向非连接的互连网络解决方案中最常用的协议。IP 协议是为 ARPAnet 研制的网际数据报协议，后来 ISO 以此为蓝本开发了无连接的网络协议(ConnectionLess Network Protocol，CLNP)。CLNP 与 IP 的功能十分相似，差别只在于个别细节和分组格式不同。

实际上，网际协议要解决的问题与网络层协议类似。在网际层提供路由信息的手段仍然是路由表。每个站或路由器都有一个网际路由表，表的每一行说明与一个目标站对应的路由器地址。网际地址通常采用“网络.主机”的形式，其中网络部分是子网的地址编码，主机部分是子网中主机的地址编码。

5.2.3 IP 协议

因特网(Internet)是目前世界上最大的计算机网络，几乎覆盖了整个世界。Internet 实际



上是一个网联网，是多个网络互连而形成的逻辑网络。希望接入 Internet 的用户首先应当接入连接 Internet 的通信子网；其次，必须执行相同的 Internet 协议软件，具有收发 Internet 协议数据报的能力；再次，还必须在 Internet 中寻找一个乐意作为信息周转的中间节点。

TCP 和 IP 是因特网中的主要协议，所以 Internet 协议也叫 TCP/IP 协议簇。IP 协议是 Internet 中的网络层协议，提供无连接服务。

5.2.3.1　IP 协议提供的服务

IP 协议是因特网中的基础协议，由 IP 协议控制传输的协议单元称为 IP 数据报。IP 数据报中含有发方/收方的 IP 地址。IP 提供不可靠的、尽力的、无连接的数据包投递服务。

1. 不可靠的投递服务

IP 协议无法保证数据报投递的结果。在传输的过程中，数据报可能会丢失、重复、延迟和乱序等，但是 IP 服务的本身不关心这些结果，也不将这些结果通知收发双方。

2. 无连接的投递服务

每个数据报独立处理和传输，因此，由一台主机发出的数据报序列，可能取不同的路径，甚至其中的一部分数据报会在传输过程中丢失。

3. 尽力投递服务

IP 协议软件决不简单地丢弃数据报，只要有一线希望，就向前投递；尽力投递的另一种体现方法是 IP 协议软件执行数据报的分段，以适应具体的传输网络，数据报的合段则由最终节点的 IP 模块予以完成。

IP 数据报的投递利用了物理网络的传输能力，网络接口模块负责将 IP 数据报封装到具体网络的帧或者分组中的信息字段。

5.2.3.2　IP 地址

一个 IP 地址由网络号和主机号两部分组成，由 4 个字节共 32 位的数字串组成，这 4 个字节通常用小数点分隔，每个字节可用十进制表示，如 192.45.8.22。IP 地址也可以用二进制和十六进制表示。

1. IP 地址分类

IP 地址可分为 5 类，如表 5.1 所示。其中 A、B、C 类是常用地址。

表 5.1　Internet 的 IP 地址空间容量

IP 地址类型	第一字节十进制范围	二进制固定最高位	二进制网络位数	网 络 数	二进制主机位数	主 机 数
A 类	0～127	0	8	126	24	$2^{24}-2$
B 类	128～192	10	16	2^{14}	16	$2^{16}-2$
C 类	192～223	110	24	2^{21}	8	$2^{8}-2$
D 类	224～239	1110	组播地址			
E 类	240～255	11110	保留给实验使用			

IP 地址除了标识一台主机外，还有几种具有特殊意义的形式。

(1) 本网络的本台主机：若一个 IP 地址全由 0 组成，即 0.0.0.0，表示在本网络上的本台主机。当一台主机在运行引导程序但又不知道其 IP 地址时使用该地址。

(2) 本网络的某个主机：网络号各位全为“0”的 IP 地址，表示在这个网络中的特定主机。它用于一个主机向同网络中其他主机发送报文。

(3) 网络地址：主机号各位全为“0”的 IP 地址标识本网络的网络地址，不分配给任何主机。

(4) 直接广播地址(有时简称为广播地址)：主机号各位全为“1”的 IP 地址，不分配给任何主机，它用于将一个分组发送给特定网络上的所有主机，即对全网广播。

(5) 受限(本地)广播地址：网络号和主机号都为 1 的 IP 地址(即 255.255.255.255)。它也是对当前网络进行广播，多数是用在当一台主机在运行引导程序时，但又不知道其 IP 地址需要向服务器获取 IP，这时用该地址作为目的地址发送分组。

(6) 回送地址(Loopback Address)：A 类网络地址 127.x.x.x 是一个保留地址，用于网络软件测试以及本地进程间的通信。

如果一个组织不需要接入因特网上，但需要在其网络上运行 TCP/IP 协议，最佳选择是使用私网地址，但 Internet 中路由器一般不转发目标地址为私网地址的数据包。私网地址如表 5.2 所示。

表 5.2　私网 IP 地址空间

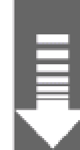
类　型	网络地址	网 络 数
A 类	10.0.0.0	1
B 类	172.16.0.0～172.31.0.0	16
C 类	192.168.0.0～192.168.255.0	256

2. 子网划分与子网掩码

由于 IP 地址的分配是以“网络”为单位进行的，如果一个部门拥有 256 个用户接入 Internet，至少应该为该部门分配两个连续的 C 类网地址。很显然，这种分配制度导致了大量的 IP 地址资源的浪费。为了提高 IP 地址的使用效率，可采用借位的方式将一个网络划分为子网：从主机号最高位开始借位变为新的子网号，所剩余的部分则仍为主机号。这使得 IP 地址的结构分为三部分：网络号、子网号和主机号。

引入子网划分技术后带来了一个重要问题，即主机路由和路由设备如何判断一个给定的 IP 地址是否已经进行了子网划分，从而能正确地从 IP 地址中分离出有效的网络标识。通常，将未引入子网划分技术前的 A、B、C 类地址称为有类别(Classful)的 IP 地址，将引入子网划分技术后的 IP 地址称为无类别(Classless)的 IP 地址，并因此引入子网掩码来描述 IP 地址中关于网络标识和主机号位数的组成情况。

子网掩码(Subnet Mask)通常与 IP 地址配对出现，其功能是告知主机或路由设备，IP 地址的哪一部分代表网络号部分，哪一部分代表主机号部分。子网掩码使用与 IP 地址相同的编码格式，长 32 位，由一串 1 和跟随的一串 0 组成。子网掩码中的 1 对应于 IP 地址中的网络号 net-id 和子网号 subnet-id，而子网掩码中的 0 对应于 IP 地址中的主机号 host-id。要得到网络或子网地址，只需将 IP 地址和子网掩码按位进行“与”运算就可以得到。



子网掩码有两种表示方法，具体如下。

(1) 用点分十进制表示法表示，如 255.255.255.0、255.255.255.240 等。

(2) 在 IP 地址后加一个“/网络号和子网号的位数”。例如，210.45.12.58/28 就表示该 IP 地址的网络号 net-id 和子网号 subnet-id 共占用 28 位，主机号占用 32−28=4 位。如果用点分十进制表示法表示，则子网掩码为 255.255.255.240，其二进制表示为：11111111 11111111 11111111 11110000。

采用子网掩码是对网络编址的有益补充，但是还存在着一些缺陷，如划分的子网中较小的会浪费许多地址。为了解决这个问题，避免任何可能的地址浪费，就出现了可变长子网掩码(Variable Length Subnetwork Mask，VLSM)的编址方案。VLSM 允许一个网络使用不同的网络掩码以适应不同规模的子网要求。

5.2.3.3　IPv4 协议

1. IPv4 数据报格式

目前因特网上广泛使用的 IP 协议为 IPv4，其数据报格式如图 5.3 所示。IPv4 协议的设计目标是提供无连接的数据包尽力投递服务。

0	4	8	16		31
版本号	IP头长度	服务类型	IP数据报长度		
标识符			标志	段偏移	
生存期		协议	报头检验和		
源IP地址					
宿IP地址					
IP选项					填充域
数据域					

图 5.3　IPv4 数据报格式

IP 数据报包括 IP 数据报报头和数据域两部分，报头主要包含数据报传输时所用的控制信息，数据域携带用户希望传输的数据信息。

- 版本号：说明对应 IP 协议的版本号(此处取值为 4)。
- IP 头长度：以 32 位字为单位的 IP 数据报报头的长度。
- 服务类型：说明本数据报对传输网络的性能要求，或者指导路由器选择适合的传输网络。前 3 位表示本数据报的优先级(取值为 0 表示一般数据，取值为 7 表示网络控制信息)；第 4～6 位分别为延迟(D)、吞吐量(T)和可靠性(R)标志位；最后两位保留未用。
- IP 数据报长度：说明整个 IP 数据报的长度，以字节为单位，最大值为 65 535。
- 标识符：唯一地标识该份 IP 数据报。IP 模块提供尽力投递的服务，在 IP 数据报投递的过程中，可能执行数据报分段的工作，将一个体积较大的数据报划分为若干小的数据报。为了便于收方 IP 模块的组装，所有小数据报的标识符域具有相同的值。
- 标志：说明本数据报是否允许分段。本域共占 3 位，从左至右第 1 位保留未用，第 2 位(DF)表示是否允许分段，第 3 位(MF)表示本分段是否为最后一段。
- 段偏移：说明本数据报分段在整个数据报中的起始位置。由于段偏移域共占 13 位，

表示源发节点发送的IP数据报最多允许有8192个分段。

- 生存期：说明本IP数据报在网络中允许停留的时间。为了避免IP数据报在网络中无限制地转发，设置了本字段。通常本字段由源发端设置，并且，每经过一个路由器(分析IP数据报)，数值减1。结果为0，则丢弃本数据报。
- 协议：说明其上层用户协议，如TCP、UDP等。
- 报头检验和：用于路由器检测IP数据报报头的正确性。该域的值在IP数据报途经的每个路由器上重新生成，并由下一跳的路由器验证。IP 模块丢弃报头出错的数据包，并通过ICMP(因特网控制消息协议)告知发送方。
- 源/宿IP地址：填写本IP数据报的发送方和接收方的IP地址。
- IP选项：用于对IPv4的功能扩充。
- 填充域：保证整个IP数据报报头的长度为32位字的整数倍。如果报头长度不是32位的整数倍，则需要在填充域中加0凑齐。

2. 数据报的分段与重装配

IP 数据报从源主机交付给目的主机，可能需要跨越多个网络，每个网络的 MTU(最大传输单元)可能不同，可能需要将一个数据报划分成若干更小的单元。数据报可以被主机或其路径中任何一台路由器分段，但数据报的重装只能在目的主机上进行。

在IP数据报报头中，标志和段偏移字段与控制分段和重装有关。标志字段由3位组成，前两位一般不用，通常设为0；最后一位是结束分段标志，标识该数据报是否是原IP数据报的最后一个分片，如果设为1则表示该数据报之后还有原数据报的分段，如果设为0则表示该数据报是原数据报的最后一个分段。段偏移字段的值表示该分段的数据相对原IP数据报的数据偏移量，该偏移量从 0 开始计算。在数据报的目的主机上，可以根据标志字段和段偏移字段判断一个IP数据报是否被分段，是否是原IP数据报的最后分段。

3. IP路由

IP数据报的传输可能需要跨越多个子网，不同的子网由IP地址中的网络标识符和子网屏蔽码标识。习惯上，子网的划分保证每个子网限定于同一个物理网络，路由器或者多网卡主机实现了不同子网之间的互连。跨越子网的IP数据报传送由IP路由算法予以控制。IP路由算法的描述如下。

IP模块根据IP数据报中的收方IP地址确定是否为本子网投递。

(1) 如果为本网投递(收发方的IP地址具有相同的IP网络标识)，利用ARP，取得对应IP地址的物理地址，形成物理帧(或分组)，IP数据报填入其数据域，直接将帧(或分组)发往目的地；结束IP路由算法。

(2) 如果为跨网投递(收发方的IP地址具有不同的NetID)，利用ARP，取得因特网网关的IP地址对应的物理地址，形成物理帧(或分组)，IP数据报填入其数据域，直接将帧(或分组)发往该网关；网关软件取出IP数据报，并重复IP路由算法。

5.2.3.4 ICMP

ICMP是IP协议的附属协议，属于网络层协议，其报文封装在IP协议数据单元中进行传送，主要用于网络设备和节点之间的控制和差错报告报文的传输。

ICMP 报文分为 ICMP 报文头部和 ICMP 报文体部两个部分。ICMP 报文的前 4 个字节是统一的格式，共有 3 个字段，即类型字段(表示差错的类型)、代码字段(表示差错的原因)、校验和(表示整个 ICMP 报文的校验结果)。其后面是数据字段，其长度取决于 ICMP 的类型。

下面将解释常用的 ICMP 报文的含义。

- 目标不可到达(类型 3)：如果路由器判断出不能把 IP 数据报送达目标主机，则向源主机返回这种报文。另一种情况是目标主机找不到有关的用户协议或上层服务访问点，也会返回这种报文。
- 超时(类型 11)：路由器发现 IP 数据报的生存期已超时，或者目标主机在一定时期内无法完成重装配，则向源端返回这种报文。
- 源抑制(类型 4)：如果路由器或目标主机缓冲资源耗尽而必须丢弃数据报，则每丢弃一个数据报就向源主机发回一个源抑制报文，这时源主机必须减小发送速度。另外一种情况是系统的缓冲区已用完，并预感到行将发生拥塞，则发出源抑制报文。
- 参数问题(类型 12)：如果路由器或主机判断出 IP 头中的字段或语义出错，则返回这种报文，报文头中包含一个指向出错字段的指针。
- 路由重定向(类型 5)：路由器向直接相连的主机发出这种报文，告诉主机一个更短的路径。
- 回声(请求/响应，类型 8/0)：用于测试两个节点之间的通信线路是否畅通。收到回声请求的节点必须发出回声响应报文。该报文中的标识符和序列号用于匹配请求和响应报文。当连续发出回声请求时，序列号连续递增。常用的 ping 工具就是这样工作的。
- 时间戳(请求/响应，类型 13/14)：用于测试两个节点之间的通信延迟时间。请求方发出本地的发送时间，响应方返回自己的接收时间和发送时间。
- 地址掩码(请求/响应，类型 17/18)：主机可以利用这种报文获得它所在的 LAN 的子网掩码。首先主机广播地址掩码请求报文，同一 LAN 上的路由器以地址掩码响应报文回答，告诉请求方需要的子网掩码。

5.2.4　TCP 和 UDP

在 TCP/IP 协议簇中有两个传输协议：传输控制协议(Transmission Control Protocol，TCP)和用户数据报协议(User Datagram Protocol，UDP)。

5.2.4.1　TCP

IP 协议提供不可靠、无连接和尽力投递的服务，构成了因特网数据传输的基础。以此为基础，TCP 协议软件增加了确认-重发、滑动窗口和复用/解复用等机制，提供面向连接的、可靠的、流投递服务。

1. TCP 协议的特性

TCP 协议在 IP 协议软件提供的服务的基础上，支持面向连接的、可靠的、面向流的投递服务。

1) 面向流的投递服务

应用程序之间传输的数据可被视为无结构的字节流(或位流)，流投递服务保证收发的字节顺序完全一致。

2) 面向连接的投递服务

流传输之前，TCP 收发模块之间需建立连接(类似虚电路)，其后的 TCP 报文在此连接基础上传输。TCP 连接报文通过 IP 数据报进行传输，由于 IP 数据报的传输导致 ARP 地址映射表的产生，从而保证了后续的 TCP 报文可以具有相同的路径。

3) 可靠的传输服务

发送方 TCP 模块在形成 TCP 报文的同时，形成一个所谓“累计核对”。“累计核对”类似于校验和，并随同 TCP 报文一起传输。接收方 TCP 模块根据该校验和判断传输的正确性：如果传输不正确，接收方简单地丢弃该 TCP 报文；否则进行应答。发送方如果在规定的时间内未能获得应答报文，则自动进行重传动作。

4) 缓冲传输

为了保证数据传输的效率，TCP 模块提供强制性传输(立即传输)和缓冲传输两种手段。缓冲传输允许将应用程序的数据流积累到一定的体积，形成报文，再进行传输。

5) 全双工传输

TCP 模块之间可以进行全双工的数据流交换。

6) 流量控制

TCP 模块提供滑动窗口机制，支持收发 TCP 模块之间的端到端流量控制。

2. TCP 报文段

TCP 报文段分为头部和数据两部分。TCP 报文段头部的前 20 个字节是固定的，后面 4*n* 个字节是可选项(*n* 为整数)，如图 5.4 所示。

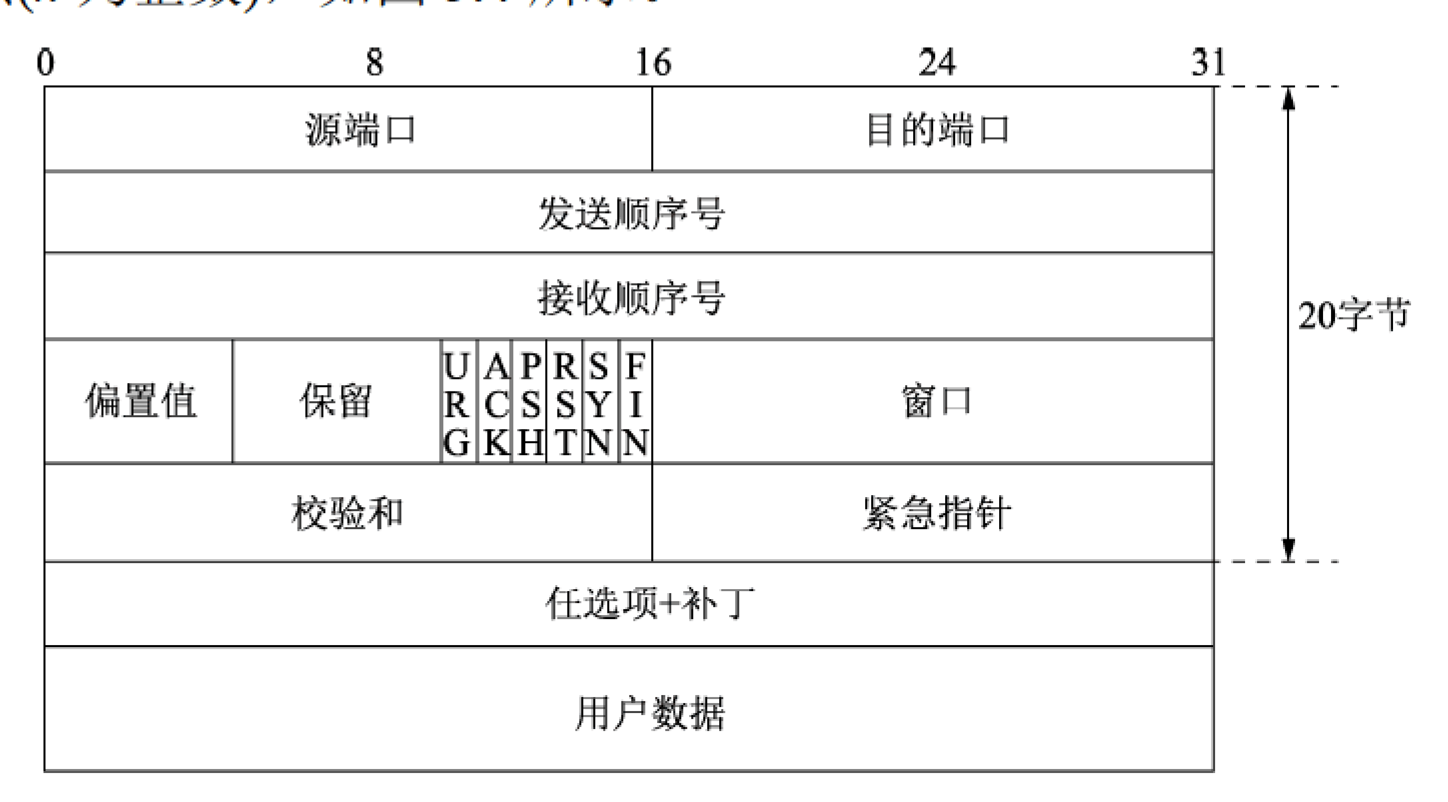


图 5.4 TCP 报文段

- 源端口(16 位)：说明源服务访问点。
- 目的端口(16 位)：表示本地服务访问点。
- 发送顺序号(32 位)：本段中第一个数据字节的顺序号。
- 接收顺序号(32 位)：捎带应答的顺序号，指明接收方期望接收的下一个数据字节的序号。
- 偏置值(4 位)：指出该段中数据的初始位置(以 32 位为单位)。



- 标志字段(6 位)：表示各种控制信息。其中各标志的含义如下。
  - URG：紧急指针字段有效标志。
  - ACK：确认号字段有效标志。
  - PSH：PUSH 操作的标志。
  - RST：要求异常终止通信连接的标志。
  - SYN：建立同步连接的标志。
  - FIN：本地数据发送已结束，终止连接的标志。
- 窗口(16 位)：本地接收窗口尺寸，即本地接收缓冲区大小。
- 校验和(16 位)：段中所有 16 位字按模 $2^{18}-1$ 相加的和，然后取 1 的补码。
- 紧急指针(16 位)：从发送顺序号开始的偏置值，指向紧急数据的最后一个字节。
- 任选项(可变)：提供任选的服务。
- 补丁(可变)：保证 TCP 段头以 32 位为边界对齐。

3. TCP 端口

TCP 模块以 IP 模块为传输基础，同时又可向多种应用程序提供传输服务。为了能够区分出对应的应用程序，便引入了 TCP 端口的含义。

TCP 端口类似于 OSI 中的传输层服务访问点，与一个 16 位的整数值相对应，该整数值也被称为 TCP 端口号。需要服务的应用进程与某个端口号进行连接，此时，TCP 模块就可以通过该 TCP 端口与应用进程通信。

由于 IP 地址可以对应到因特网中的某台主机，而 TCP 端口号可对应到主机上的某个应用进程，因此，TCP 模块采用 IP 地址和端口号的对偶来标识 TCP 连接的端点。一条 TCP 连接实质上对应了一对 TCP 端点。

4. TCP 连接建立与释放

(1) 建立连接：采用“三次握手”的方法，其目的是保证双方都相互知道对方已准备好进行数据传输，双方确认一个数据传输的初始序列号，防止产生错误的连接，如图 5.5(a)所示。

(2) 释放连接：使用了四次握手过程，如图 5.5(b)所示。

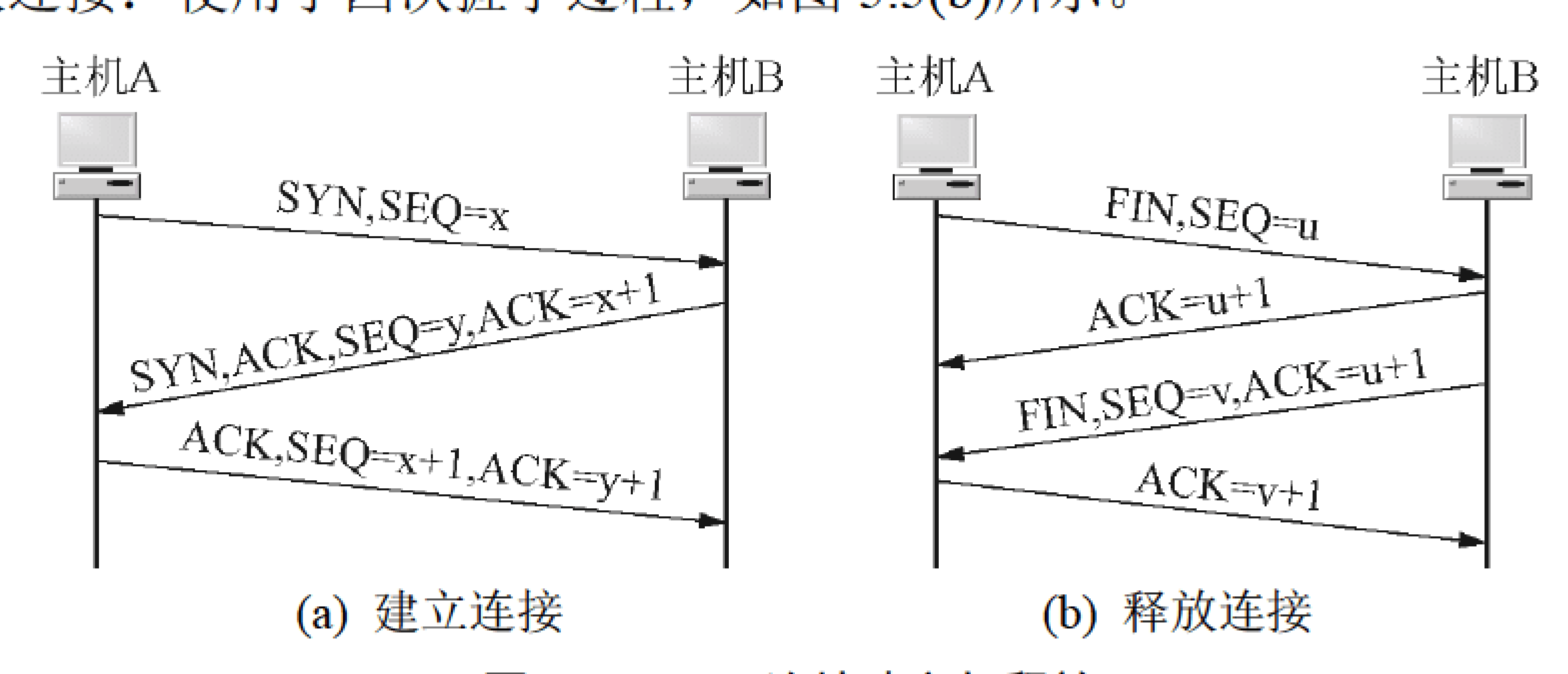


图 5.5　TCP 连接建立与释放

5. 窗口机制

TCP 采用了具有重传功能的肯定确认技术作为可靠数据流传输服务的基础。

为了提高数据流传输过程的效率，在上述基础上引入了滑动窗口协议，它允许发送方在等待一个确认之前可以发送多个分组。滑动窗口协议规定只需重传未被确认的分组，且

未被确认的分组数最多为窗口的大小。TCP 允许随时改变窗口大小，通过通告值来说明接收方还能再接收多少数据。通告值增加，发送方扩大发送滑动窗口；通告值减小，发送方缩小发送滑动窗口。

滑动窗口协议的处理过程如下。

(1) TCP 连接阶段，双方协商窗口尺寸，同时接收方预留数据缓存区。

(2) 发送方根据协商的结果，发送符合窗口尺寸的数据字节流，并等待对方的确认。

(3) 接收方根据当前的处理能力，调整接收窗口的尺寸，并在确认中告知发送方。

(4) 发送方根据确认信息，改变窗口的尺寸，增加或者减少发送未得到确认的字节流中的字节数。调整过程包括：如果出现发送拥塞，发送窗口缩小为原来的一半，同时将超时重传的时间间隔扩大一倍。

5.2.4.2 UDP

UDP(User Datagram Protocol，用户数据报协议)是无连接、不可靠的数据包投递服务，常用于数据量较小的数据传输。UDP 报文段如图 5.6 所示。



图 5.6 UDP 报文段

UDP 的优点：在少量数据传输时，可以减少 TCP 连接的过程，提高工作效率。

UDP 的不足：用户应用程序必须负责解决数据报排序、差错确认等问题。

在多媒体应用中，常用 TCP 支持数据传输，UDP 支持音频/视频传输。

5.2.4.3 端口号

1. 端口号分类

保留端口：范围是 1～1023，固定分配给一些常用的应用层协议使用。目前，保留端口的端口号已经被广大网络应用者接受，形成了标准，如表 5.3 所示。

表 5.3 常用的保留端口号

端 口 号	传输层协议	用 途	说 明
20	TCP	FTP，数据	文件传输协议(数据连接)
21	TCP	FTP，控制	文件传输协议(控制连接)
23	TCP	TELNET	远程终端
25	TCP	SMTP	简单邮件传输协议
53	TCP/UDP	DNS	域名系统
67	UDP	BOOTP/DHCP，服务器	动态主机配置协议服务器端口
68	UDP	BOOTP/DHCP，客户机	动态主机配置协议客户机端口
69	UDP	TFTP	简单文件传输协议

续表

端 口 号	传输层协议	用　途	说　明
80	TCP	HTTP	超文本传输协议
110	TCP	POP3	邮局协议
111	TCP	RPC	远程过程调用
161	UDP	SNMP	简单网络管理协议
162	UDP	SNMP(trap)	简单网络管理协议(陷阱)

注册端口：范围是 1024～49 151，不指派，但需要在 IANA 注册以防止重复。

动态端口：范围是 49 152～65 535，用来随时分配给请求通信的客户进程使用，是短暂端口。

2. 套接字地址

套接字地址将一个 IP 地址与一个端口号结合起来。客户套接字地址唯一地定义了客户进程，服务器套接字地址唯一地定义了服务器进程。

5.2.5　地址解析协议

在局域网中，实际传输的是“帧”，帧里面是有目标主机的 MAC 地址的。在以太网中，一个主机要和另一个主机进行直接通信，必须知道目标主机的 MAC 地址。但这个目标 MAC 地址是如何获得的呢？它就是通过地址解析协议获得的。

5.2.5.1　ARP

ARP(Address Resolution Protocol)的功能是通过目标主机的 IP 地址，查询目标主机的 MAC 地址，实现了 IP 地址与 MAC 地址的映射，保证通信的顺利进行。

ARP 使用一种询问/回答机制。如果主机 H1 要发送一个 IP 数据报给主机 H4，但它只知道 H4 的 IP 地址 P4，而不知道它的 MAC 地址，则按照图 5.7 所示的过程发送数据包。

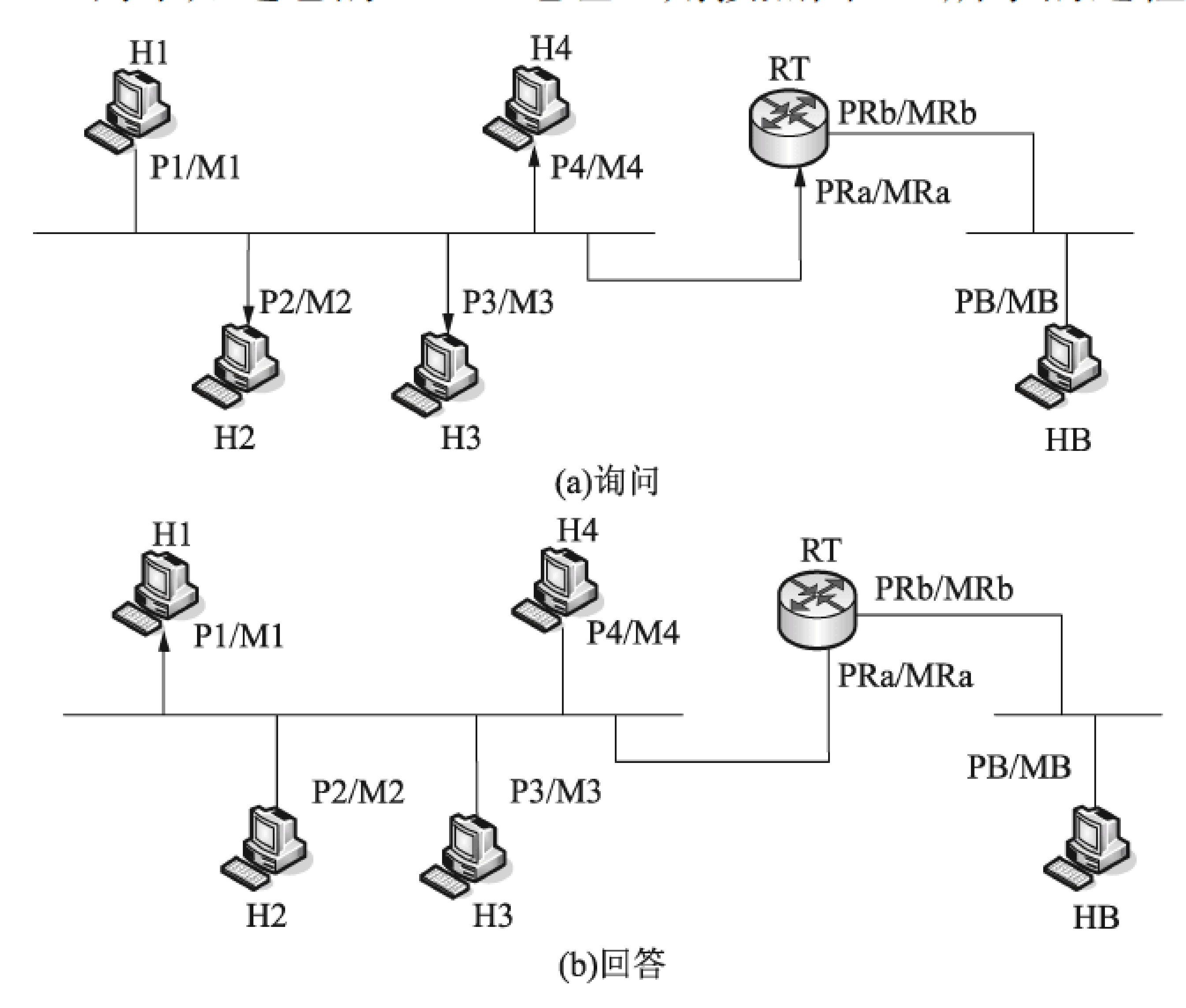


图 5.7　地址解析过程

(1) H1 构造好 IP 数据报后，由于它不知道发放哪个 MAC 地址，还不能将其交给网卡处理。这时 H1 先构造一个 ARP 请求数据报，该数据报中包含了 H4 的 IP 地址 P4，并留下一个空位表示 H4 的 MAC 地址。H1 的 ARP 将该数据报交给网卡，让它将该数据报作为广播帧发送出去。

(2) 网络中的所有网卡收到该广播帧后将帧中的数据取出交给上层 ARP 处理。

(3) ARP 在收到这个请求数据报后将自己的 IP 地址与数据报中的 IP 地址进行比较，如果相同就表示对方在询问自己的 MAC 地址。如果发现不是询问自己的 MAC 地址，ARP 就会丢弃该数据报。

(4) 只有 H4 会处理这个 ARP 请求数据报。这时 H4 将自己的 MAC 地址填在 MAC 地址空位上，并将该数据报改为 ARP 响应数据报。由于 H1 在发送的请求数据报中填写了自己的 MAC 地址和 IP 地址，因此 H4 让网卡将 ARP 响应数据报以单播方式发送给主机 H1。

对于不在同一以太网的通信，该过程略有不同。例如，H1 要与 HB 通信，H1 知道它与 HB 不在同一网络中，需要通过路由器将数据报发送给 HB，因此 H1 将 IP 数据报发送给路由器 RT。RT 将数据报转发给 HB 时，如果它不知道 HB 的 MAC 地址，它也会使用 ARP 协议进行询问。

如果每次发送一个 IP 数据报都需要进行一次 ARP 请求数据报的广播，那么发送一个 IP 数据报的代价是很高的。因此，通常在系统中维持一个 ARP 缓存，以减少地址解析所需的通信。

5.2.5.2 RARP

RARP(Reverse Address Resolution Protocol)是反向地址解析协议，其作用是将 MAC 地址转换为 IP 地址。某些主机(通常是无盘工作站)只知道自己的 MAC 地址，但有时候需要知道其 IP 地址，这就需要用到 RARP 协议。为了使 RARP 正常工作，在局域网中至少有一台主机充当 RARP 服务器，并且要在 RARP 服务器中建立好 MAC 地址与 IP 地址的映射表。

5.2.6 网关协议

Internet 中的路由器叫作 IP 网关。网关协议用于网关之间交换路由信息。

5.2.6.1 自治系统

自治系统是由同构型的网关连接的互联网，这样的系统往往是由一个网络管理中心控制的。自治系统内部的网关之间执行内部网关协议(IGP)，互相交换路由信息。IGP 是自治系统内部专用的，为特定的应用服务，在自治系统之外是无效的。

一个互联网也可能由不同的自治系统互连而成。在这种情况下，不同的自治系统可能采用不同的路由表和不同的路由选择算法。在不同自治系统中的网关之间交换路由信息，要用外部网关协议(EGP)。EGP 比 IGP 传送的信息要少一些，因为 EGP 只涉及自治系统之间的路由信息，而与系统内部的路由无关。EGP 以自治系统为节点，通告各个网关可到达哪些系统。

5.2.6.2 外部网关协议

自治系统之间使用 EGP，最新的 EGP 叫作边界网关协议(BGP)。BGP 的主要功能是控

制路由策略，如是否愿意转发过路的分组等。BGP 的报文通过 TCP 连接传送。BGP 报文可实现以下 3 个功能过程。

(1) 建立邻居关系：位于不同自治系统中的两个路由器首先要建立邻居关系，然后才能周期性地交换路由信息。建立邻居关系的过程是一个路由器发送 Open 报文，另一个路由器若愿意接受请求，则以保持活动状态报文应答。

(2) 邻居可达性：这个过程维护邻居关系的有效性。通过周期性地互相发送 KeepAlive 报文，双方都知道对方的活动状态。

(3) 网络可达性：每个路由器保持一个数据库，记录着它可到达的所有子网。当情况有变化时，用更新报文把最新信息及时地广播给所有实现 BGP 的路由器。

5.2.6.3　内部网关协议

Internet 的内部路由协议经过了几次大的变化。最初的 RIP(路由信息协议)是基于 Bellman-Ford 算法的延迟矢量协议。这个协议在网络规模不大时工作得较好，但当网络规模扩大后，因为交换的路由信息太多而显得效率很低。于是，在 1979 年 5 月它被另一个路由协议——基于 Dijkstra 算法的链路状态协议所取代。从 1988 年开始，IETF 开始研制新的路由协议，这就是 OSPF(开放最短路径优先)协议。1990 年，OSPF 正式成为新的内部路由协议标准。

1. RIP

路由信息协议(RIP)是一种基于距离矢量算法的路由协议，属于内部网关协议。它通过计算抵达目的地的最少跳数(Hop)来选取最佳路径，默认每 30 秒向其相邻设置发出一个包含整个路由表副本的 RIP 更新信息。RIP 的跳数最多计算到 15 跳，当超过这个数字时，RIP 会认为目的地不可达。由于单纯地以跳数作为选路的依据而不能充分描述路径特性，可能会导致所选的路径不是最优，因此 RIP 只适用于中小型网络。

RIP 包括 RIPv1 和 RIPv2 两个版本，RIPv1 不支持变长子网掩码(VLSM)；RIPv2 支持变长子网掩码(VLSM)，同时 RIPv2 支持明文认证和 MD5 密文认证。RIPv1 使用广播发送报文。RIPv2 有两种传送方式，即广播方式和组播方式，默认采用组播发送报文，组播地址为225.0.0.9。

2. OSPF 协议

OSPF 基本上仍是一种链路状态协议。OSPF 的路由器维护一个本地链路状态表，并随时向其他相邻的路由器发送关于链路状态的更新信息。通过周期地扩散传播链路状态信息，每个路由器都记住了关于网络拓扑结构的全局数据库。同时 OSPF 路由器根据用户指定的链路费用标准(延迟、带宽或收费率等)计算最短通路，由到达各个目标的最短通路构成路由表。OSPF 报文包含在原始的 IP 数据报中传送。

为了使 OSPF 协议能够用于规模很大的网络，OSPF 协议将一个自治系统再划分为若干更小的范围，每一个区域都有一个 32b 的区域标识符(用整数或点分十进制表示)。OSPF 协议使用层次结构的区域划分。在上层的区域叫作主干区域(Backbone Area)，主干区域的标识符规定为 0.0.0.0。主干区域的作用是连通其他在下层的区域。如果一个路由器端口被分配到多个区域中，这个路由器就被称为区域边界路由器(Area Border Router，ABR)，它是那些处在区域边缘的连接了多个区域的路由器。

3. IGRP

IGRP(内部网关路由协议)是一种基于距离矢量的内部路由协议，用于一个AS内传递路由信息，是Cisco路由器专用协议。

IGRP的特点如下。

- 使用组合用户度量尺度，包括延迟、带宽、可靠性和负载。
- 不支持VLSM和不连续子网。
- 在默认情况下，每90s发送一个路由更新广播，在3个更新周期(即270s)内，若没有接收到一个路由器的更新广播，则宣布路由不可访问，7个更新周期(即630s)后，将从路由表中清除路由。

5.2.6.4 核心网关协议

Internet中有一个主干网，所有的自治系统都连接到主干网上。主干网中的网关叫核心网关。核心网关之间交换路由信息时使用网关到网关协议(GGP)。这里需要区分 EGP 和GGP，EGP用于两个不同自治系统中的网关之间交换路由信息，而GGP是主干网中的网关协议。因为主干网中的核心网关是由InterNOC(网络操作中心)直接控制的，所以GGP更具有专用性。当一个核心网关加入主干网时用GGP向邻机广播发送它所连接的网络的路由信息，各邻机更新路由表，并进一步传播新的路由信息。

GGP的报文分为以下4类。

- 路由更新报文：发送路由信息。
- 应答报文：对路由更新报文的应答，分肯定和否定两种。
- 测试报文：测试相邻网关是否存在。
- 网络接口状态报文：测试本地网络连接的状态。

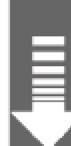
5.2.7 路由器技术

在因特网的发展过程中有很多问题要解决。IP 地址短缺是问题之一，其短期解决方案是在IPv4路由器上实现网络地址翻译NAT和无类别的域间路由技术等，长期解决方案是使用IPv6技术。随着网络规模的扩大，路由器逐渐成为网络通信的瓶颈，解决这个问题的主要技术被归纳为第三层交换技术。

5.2.7.1 NAT技术

NAT技术主要解决IP地址短缺的问题。最初提出的建议是在子网内部使用局部地址，而在子网外部使用少量的全局地址，通过路由器进行内部和外部地址的转换。局部地址是在子网内部独立编址的，可以与外部地址重叠。这种想法的基础是假定在任何时候子网中只有少数计算机需要与外部通信，可以让这些计算机共享少量的全局IP地址。后来根据这种技术又开发出其他一些应用，如动态地址翻译、伪装等。

- 动态地址翻译的好处是节约了全局IP地址，而且不需要改变子网内部的任何配置，只需在边界路由器中设置一个动态地址变换表就可以工作了。
- 伪装技术使用一个路由器的IP地址就可以把子网中所有主机的IP地址都隐藏起来。



5.2.7.2 CIDR 技术

1. 无分类域间路由选择

无分类域间路由选择(CIDR)消除了传统 A 类、B 类和 C 类地址以及划分子网的概念，从而更加有效地分配 IPv4 的地址空间。CIDR 使用各种长度的“网络前缀”(Network-Prefix)来代替分类地址中的网络号和子网号，而不像分类地址中只使用 1 字节、2 字节和 3 字节长的网络号。CIDR 不再使用“子网”概念而使用网络前缀，使 IP 地址从三级编址(使用子网掩码)又回到两级编址，但这是一个无分类的两级编址。CIDR 使用“斜线记法”，它又称为 CIDR 记法，即在 IP 地址后面加上一斜线“/”，然后写上网络前缀所占的比特数(这个数值对应于三级编址中子网掩码中比特 1 的个数)。例如，128.15.146.158/20，表示在这 32 比特中，前 20 比特表示网络前缀，而后面的 12 比特为主机号。

CIDR 将网络前缀都相同的连续的 IP 地址组成“CIDR 地址块”。一个 CIDR 地址块是由地址块的起始地址(即地址块中地址块数值最小的一个)和地址块中的地址数来定义的。CIDR 地址块也可用斜线记法来表示，例如，128.15.32.0/20 表示地址块共有 2^{12} 个地址，而这个地址块的起始地址是 128.15.32.0。

2. 超网

超网技术是将几个小的网络组成一个大的网络。例如，一个组织需要 1000 个地址，申请了 4 个 C 类地址，可以把 4 个 C 类地址合并为一个超网，如图 5.8 所示。CIDR 技术实现了超网。

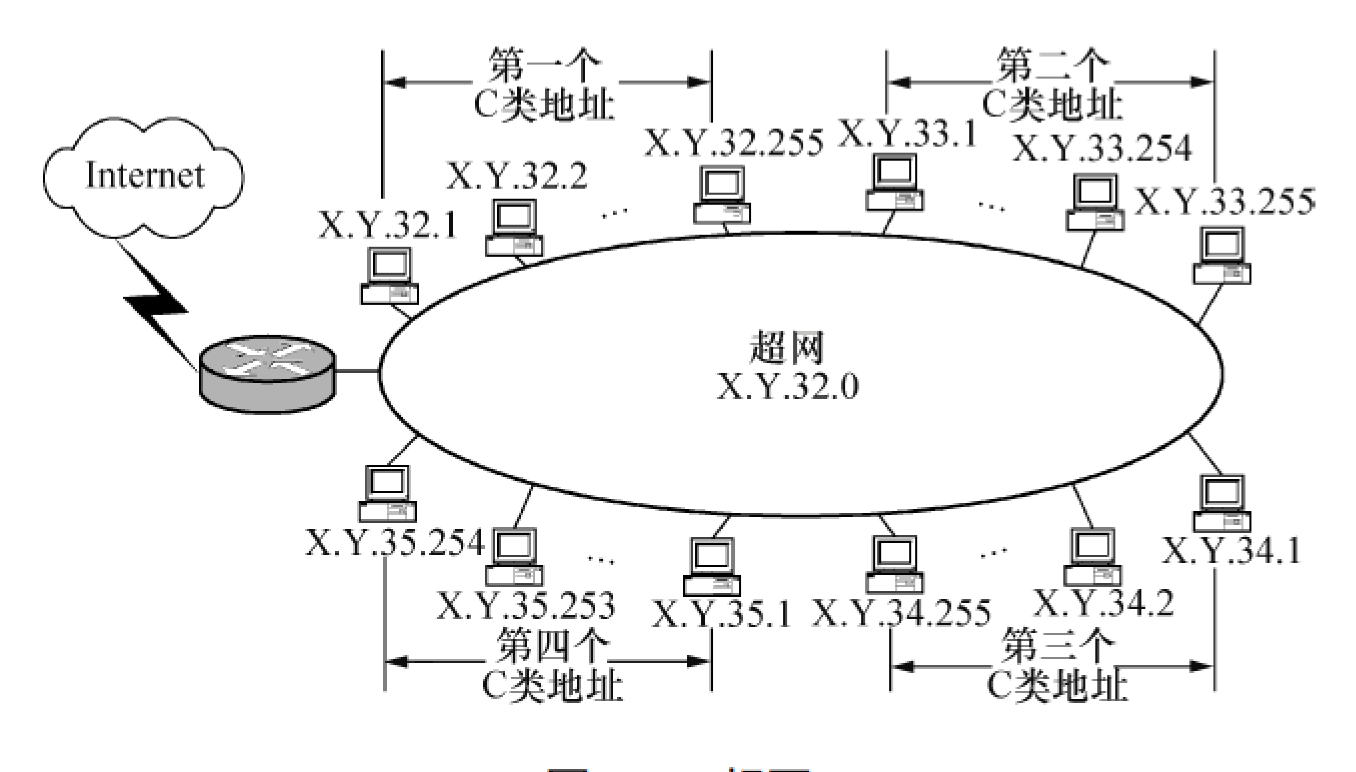


图 5.8 超网

3. 路由汇总

路由汇总也称路由聚合，其实现方法与超网相同，但它的主要目的是减少路由表的网络数目，减轻路由器的负担。在大型的网络中，可能包含几十万条 IP 路由，有些存储容量较小的路由器无法容纳如此庞大的路由信息，而使用路由汇总可以合并几个网络地址为一个代表这几个网络的总结网络地址。

设有 172.18.129.0/24、172.18.130.0/24、172.18.132.0/24 和 172.18.133/24 四条路由，进行路由汇聚，能覆盖这 4 条路由的地址是 172.18.128.0/21。计算方法是找出 4 条路由的网络地址的共同前缀和位数，计算过程如图 5.9 所示。

172.18.129.0/24	→	10101100	00010010	10000	001	00000000
172.18.130.0/24	→	10101100	00010010	10000	010	00000000
172.18.132.0/24	→	10101100	00010010	10000	100	00000000
172.18.133/24	→	10101100	00010010	10000	101	00000000
相同位 21	→	10101100	00010010	10000	000	00000000
		(172)	(18)	(128)		(0)

图 5.9　路由汇聚的过程

5.2.7.3　第三层交换技术

1. 三层交换机

所谓第三层交换，是指利用第二层交换的高宽带和低延迟优势尽快地传送网络层分组的技术。交换和路由不同，前者用硬件实现，速度快；而后者由软件实现，速度慢。三层交换机的工作原理可以概括为：一次路由，多次交换。就是说，当三层交换机第一次收到一个数据包时必须通过路由功能寻址转发端口，同时记住目标 MAC 地址和源 MAC 地址，以及其他有关信息，当再次收到目标地址和源地址相同的帧就直接进行交换，不再调用路由功能。所以三层交换机不但具有路由功能，而且比通常的路由器转发得更快。

下面将通过一个简单的网络来介绍三层交换机的工作过程。

假设有两台主机(分别是主机 A、主机 B)挂接在三层交换机上。比如，主机 A 要给主机 B 发送数据，则三层交换机的工作过程如下。

(1) 已知目的 IP 地址，那么主机 A 就用其本身的子网掩码与该目的 IP 进行逻辑“与”运算，取得目的网络号，判断目的 IP 地址是否与自己在同一网段。

(2) 如果在同一网段，但不知道转发数据所需的 MAC 地址，主机 A 就发送一个 ARP 请求，主机 B 返回其 MAC 地址；然后，主机 A 用此 MAC 封装数据包并发送给交换机，交换机启用二层交换模块，查找 MAC 地址表，将数据包转发到相应的端口。

(3) 如果目的 IP 地址不是同一网段的，那么主机 A 要实现和主机 B 的通信，就要将第一个正常数据包发送给一个默认网关，这个默认网关一般在操作系统中已经设好，对应第三层路由模块。所以对于不是同一子网的数据，最先在数据包中目的 MAC 地址中放入的是默认网关的 MAC 地址，然后由三层模块接收此数据包，查询路由表以确定到达主机 B 的路由。构造一个新的帧头，其中以默认网关的 MAC 地址为源 MAC 地址，以主机 B 的 MAC 地址为目的 MAC 地址。通过一定的识别触发机制，确立主机 A 与主机 B 的 MAC 地址及转发端口的对应关系，并记录进三层交换机高速缓存的交换表。以后的主机 A 到主机 B 的数据，就直接交由二层交换模块完成。这就是通常所说的一次路由，多次交换。

2. MPLS

IETF 开发的多协议标记交换(Multiprotocol Label Switching，MPLS，RFC3031)把第二层的链路状态信息(带宽、延迟、利用率等)集成到第三层的协议数据单元中，从而简化和改进了第三层分组的交换过程。理论上，MPLS 支持任何第二层和第三层协议。MPLS 报头的位置介于第二层和第三层之间，可称为第 2.5 层。MPLS 可以承载的报文通常是 IP 包，当然也可以直接承载以太帧、AAL5 包，甚至 ATM 信元等。

(1) MPLS 的工作原理：为每个 IP 数据包提供一个标记，并由此决定数据包的路径以



及优先级。MPLS 是一种可以在多种第二层媒体上进行标签交换的网络技术，这一技术结合了第二层的高速交换(硬件交换)和第三层的灵活路由处理的特点。

(2) MPLS 的网络构成：由边缘标签路由器(LER)和标签交换路由器(LSR)组成，LER 构成 MPLS 网的接入部分，LSR 构成 MPLS 网的核心部分。LER 发起或终止标签交换路径(LSP)连接并完成传统 IP 数据包转发和标签转发功能。入口 LER 完成 IP 包的分类、寻路、转发表和 LSP 表的生成，以及 FEC 转发等价类至标签的映射。出口 LER 终止 LSP，并根据弹出的标签转发剩余的包。LSR 只是根据交换表完成转发功能。这样所有复杂功能都在 LER 内完成，而 LSR 只完成高速转发功能，如图 5.10 所示。

(3) MPLS 网络中各 LSR 是通过专门标记分发协议(Label Distribution Protocol，LDP)交换报文，并找出相应 LSP 的。

(4) MPLS 的工作过程如下。

① 当 IP 数据包到达 LER 时，LER 首先分析 IP 包头的信息。对于每一个 FEC，LER 根据标签信息库(LIB)为该 IP 数据包分配一个标签，并将使用该标签封装的数据包从 LIB 所规定的下一个接口发送出去。

② 当带有标签的数据包到达 MPLS 网络内部 LSR 时，LSR 提取局部标签，同时使用该标签到 LIB 查找输出标签和下一个接口，并使用输出标签代替数据包的输入标签后将新数据包从下一个接口发送出去。

③ 数据包到达 MPLS 域的另外一端，这时 LER 去掉封装的标签，仍然按照 IP 包的路由方式将数据包继续传送到目的地。

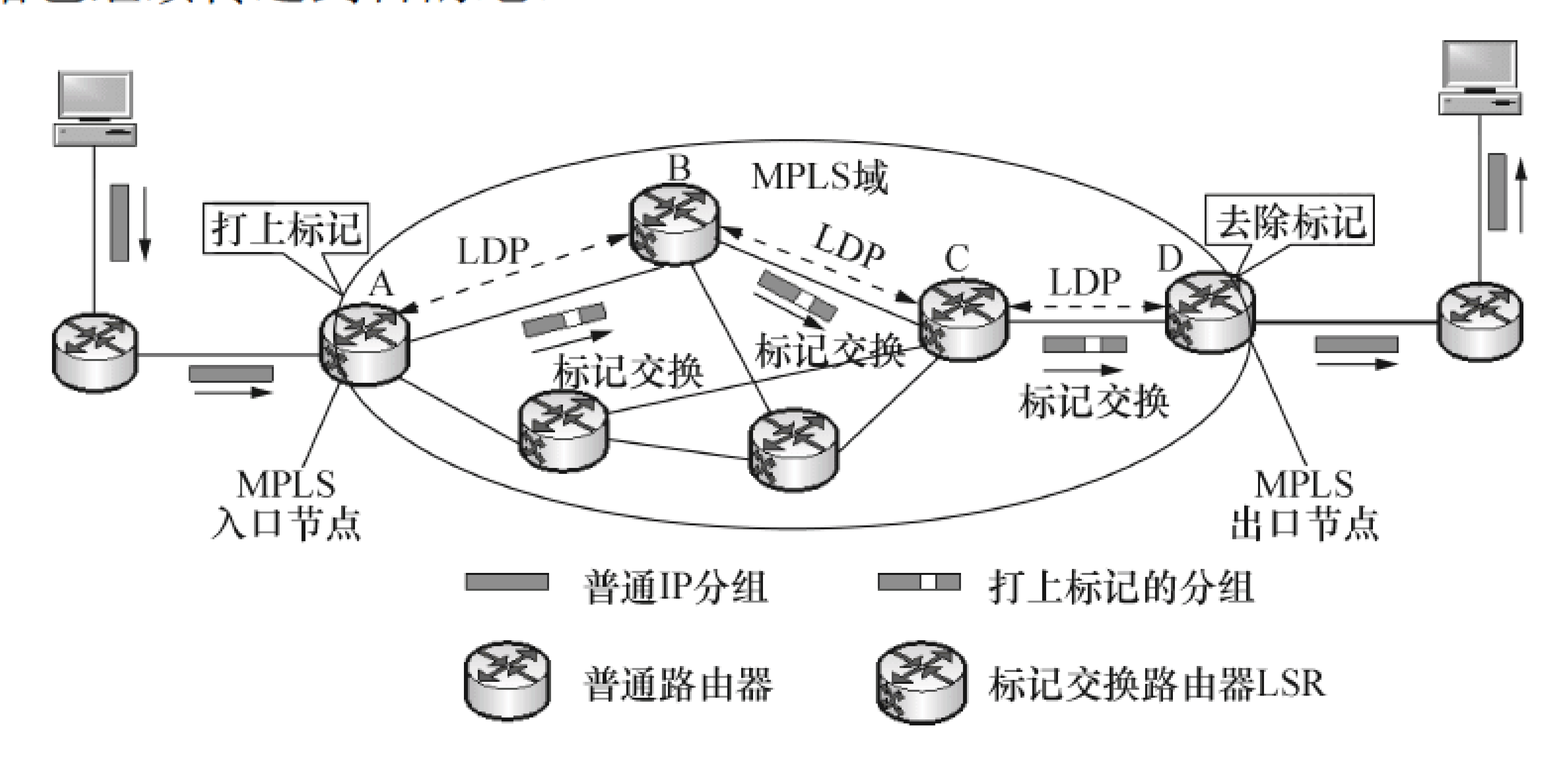


图 5.10　MPLS 的基本原理

5.2.8　IP 组播技术

5.2.8.1　组播模型概述

由一个源向一组主机发送信息的传输方式称为组播(Multicast)。每一个组播组被指定了一个 D 类地址作为组标识符。组播源利用组地址作为目标地址来发送分组，组播成员向网络发出通知，声明它期望加入的组的地址。IGMP (Internet Group Management Protocol)用于支持接收者加入或离开组播组。一旦有接收者加入了一个组，就要为这个组在网络中构建一个组播分布树。

实现 IP 组播的前提是组播源和组成员之间的下层网络必须支持组播，包括下面的支持功能。

- 主机的 TCP/IP 实现支持 IP 组播。
- 主机的网络接口支持组播。
- 需要一个组管理协议，使得主机能够自由地加入或离开组播组。
- IP 地址分配策略能够将第三层组播地址映射到第二层 MAC 地址。
- 主机中的应用软件应支持 IP 组播功能。
- 所有介于组播源和组成员之间的中间节点都支持组播路由协议。

5.2.8.2 组播地址

通常有两种组播地址，一种是 IP 组播地址，另一种是以太网组播地址。IP 组播地址在互联网中标识一个组，把 IP 组播数据报封装到以太帧中时要把 IP 组播地址映像到以太网的 MAC 地址，其映像方式是把 IP 地址的低 23 位复制到 MAC 地址的低 23 位。

IPv4 的 D 类地址是组播地址，其地址范围是 224.0.0.0～239.255.255.255。D 类地址被划分为 3 类。

- 224.0.0.0～224.0.0.255：保留地址，用于路由协议或其他下层拓扑发现协议以及维护管理协议等。
- 224.0.1.0～238.255.255.255：用于全球范围的组播地址分配。
- 239.0.0.0～239.255.255.255：在管理权限范围内使用的组播地址，可以在本地子网中作为组播地址使用。

为了避免使用 ARP 协议进行地址分解，IANA 保留了一个以太网地址块 0x0100.5E00.0000 用于映像 IP 组播地址，其中第 1 个字节的最低位是 I/G (Individual/Group)，应设置为“1”，以表示以太网组播，所以 MAC 组播地址的范围是 0x0100.5E00.0000～0x0100.5E7F.FFFF。

5.2.8.3 因特网组管理协议

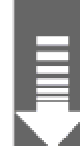
在 IPv4 环境中提供组管理的协议是 IGMP，IPv6 环境中，组管理协议已经合并到 ICMPv6 协议中。

1. IGMP 报文

RFC 3376 定义了 IGMPv3 成员资格询问和报告报文，也定义了组记录的格式，IGMP 报文封装在 IP 数据报中传输。

成员资格询问报文：

<table>
<tr><td colspan="3">类型</td><td>最大响应时间</td><td>校验和</td></tr>
<tr><td colspan="5">组地址</td></tr>
<tr><td>保留</td><td>S</td><td>QRV</td><td>QQIC</td><td>源地址数</td></tr>
<tr><td colspan="5">源地址[1]</td></tr>
<tr><td colspan="5">源地址[2]</td></tr>
<tr><td colspan="5">⋮</td></tr>
<tr><td colspan="5">源地址[N]</td></tr>
</table>



成员资格报告报文：

类型	保留	校验和
保留		组记录数
组记录[1]		
组记录[2]		
⋮		
组记录[N]		

组记录：

记录类型	辅助数据长度	源地址数
组播地址		
源地址[1]		
源地址[2]		
⋮		
源地址[N]		
辅助数据		

2. IGMP 操作

为了加入一个组，主机要发送成员资格报告报文；这个组的所有成员主机都会接收到这个分组，从而都知道了新加入的组成员。本地 LAN 中的路由器必须监听所有的 IP 组播地址，以便接收所有组成员的报告报文。

为了维护一个当前活动的组播地址列表，组播路由器要周期性地发送 IGMP 通用询问报文，封装在以 224.0.0.1(所有主机)为目标地址的 IP 数据报中。

当主机要离开一个组时，它向所有路由器(224.0.0.2)发送一个组离开报告，其中的记录类型为 EXCLUDE，源地址列表为空，其含义是该组所有的组播源都被排除。

5.2.8.4　组播路由协议

1. 组播树

建立组播树是实现组播传输的关键技术，组播树是以组播源为树根的最小生成树，沿着这个树从根到叶的方向可以把组播分组传输到所有的组成员用户，且分组在每段链路上只出现一次。

组播树分为两种。源专用树是以每一个组播源为根建立最小生成树，PIM 协议把这种树叫作最短通路树(SPT)。在组播树中使用了一种称为反向通路转发(RPF)的技术来防止组播分组在网络中循环转发。另外一种组播树是共享分布树。该方案利用了由(一个或多个)路由器组成的分布与中心来生成一棵组播树，由这棵树负责所有组播组的通信。PIM 协议称这种树为约会点树(RPT)。

2. 密集模式路由协议

密集模式路由协议假定组播成员密集地分布在整个网络中，而且网络有足够的带宽，允许周期性地通过泛洪传播来建立和维护分布布树。密集模式路由协议包括距离矢量组播路由协议(DVMRP)、组播开放最短路径优先协议(MOSPF)，以及密集模式的独立组播协议(PIM-DM)等。

PIM 引入了协议无关的概念，它可以使用任何单播路由协议(OSPF、IS-IS、BGP)建立的路由表来实现反向通路转发(RPF)检查，这是它与其他组播路由协议的主要区别。

当组播源 S 开始向组播组 G 发送数据时，组播分组被泛洪到网络中的所有区域。当一个路由器接收到组播数据报后，首先通过单播路由表进行 RPF 检查，然后剪掉不需要的分支，这一过程被称为泛洪—修剪循环，这是所有密集模式协议中使用的关键技术。

3. 稀疏模式路由协议

稀疏模式路由协议适用于带宽小、组播成员分布稀疏的互联网络。在这种网络中，泛洪传输会引起网络阻塞，所以要使用其他技术来建立组播树。CBT 协议建立了一棵为所有组播会话服务的组播树，而稀疏模式的独立组播协议 PIM-SM 既可以为每个组播组建立一个以约会点为树根的共享树，也可以为每个组播源建立一棵最短通路树。

5.2.9 IP QoS 技术

5.2.9.1 集成服务

集成服务模型的基本思想是将 RSVP (Resource Reservation Protocol，资源预留协议)作为 Int－Serv 结构中的主要信令协议，它基于每个流提供端到端的保证或是受控负载的服务。Int－Serv 使用一种类似 ATM 的 SVC(Switched Virtual Circuit，交换虚电路)的方法，它在发送方和接收方之间用 RSVP 作为每个流的信令。RSVP 信息跨越整个网络。

这种服务模型在发送报文前，需要向网络申请特定的服务。应用程序先通知网络发送报文的流量参数和所需的服务质量请求(如带宽、时延等)。应用程序在收到网络预留资源的确认信息后，才开始发送报文，发送报文被控制在流量参数规定的范围内。

5.2.9.2 区分服务

区分服务模型的基本思想是可以根据预先确定的规则对数据流进行分类，以便将多种应用数据流综合为有限的几种数据流等级。

区分服务是由综合服务发展而来的，它采用了 IETF 的基于 RSVP 的服务分类标准，抛弃了分组流沿路节点上的资源预留。

IP QoS 的业务区分结构使用 IPv4 报头中的业务类型(ToS)字段，并将 8 位 ToS 字段重新命名，作为 DS 字段，其中 6 位可供目前使用，其余 2 位以备将来使用。

5.2.9.3 流量工程

流量工程为业务流选择路径的处理过程，以在网络中不同的链路、路由器和交换机之间平衡业务流负载。

利用多协议标签交换 MPLS(Multi-Protocol Label Switching)技术，可以协助解决 QoS 问题。MPLS 是一种结合第二层和第三层的交换技术，引入了基于标签的机制，把路由选择和数据转发分开，由标签来规定一个分组通过网络的路径。MPLS 网络由核心部分的标签交换路由器(LSR)、边缘部分的标签边缘路由器(LER)组成。

由于 MPLS 采用标签交换来进行 MPLS 转发，因此其转发效率高于传统 IP 通过路由器的转发，从而通过减少转发时间来提高 QoS。此外，MPLS 的报文头中包含一个 3bit 的 EXP 字段，通过该字段可以标记该 MPLS 报文的优先级，从而使设备在转发该 MPLS 报文时能根据优先级标志进行区别对待。

5.2.10 Internet 基本服务

5.2.10.1 域名系统

1. 域名体系

IP 地址为因特网提供了统一的寻址方式，直接使用 IP 地址便可以访问因特网中的主机资源。但是，由于 IP 地址只是一串数字，没有任何意义，对于用户来说，记忆起来十分困难，所以几乎所有的因特网应用软件都不要求用户直接输入主机的 IP 地址，而是直接使用具有一定意义的主机名。采用命名机制对主机进行命名主要是为了方便用户使用互联网。命名机制要能为特定的主机在整个互联网上指定一个唯一的名字，而且名字要便于管理，能够方便地分配、确认以及回收，同时要能高效地将主机名与 IP 地址进行映射。在 TCP/IP 互联网中的名字管理机制是由域名系统(Domain Name System，DNS)来实现的。

域表示一个区域或者范围，域内可以容纳许多主机，因此并非每一台接入因特网的主机都必须具有一个域名地址，但是每一台主机都必须属于某个域，即通过该域的服务器可以查询和访问到这一台主机。通常，该域服务器称为域名服务器。对应因特网的层次结构，域采用了嵌套结构与之对应。域名地址由一系列“子域名”组成，子域名的个数通常不超过 5 个，并且，子域名之间用句点“.”分隔，从左到右子域的级别升高，高一级的子域包含低一级的子域。这种嵌套的域名结构形成一个域名树，树中的子节点和树叶标识分别表示不同的域，树叶被其上级的子节点或者树根所包含。这种域名结构也十分类似常用的通信地址(仅和我国表示地址的顺序有所不同)，符合人类表达的习惯。

一台主机的主机名应由它所属的各级域的域名与分配给该主机的名字共同构成，顶级域名放在最右面，分配给主机的名字放在最左面，各级名字之间用“.”隔开。通常其格式如下。

主机名. 机构名. 网络名. 顶层域名

例如，www.tsinghua.edu.cn 就是清华大学的 WWW 主机的域名地址。

因特网域名的取值遵守一定的规则。第一级域名通常分配给主干网节点，取值为国家名；第二级域名对应为次级节点，通常表示组网的部门或组织；二级域以下的域名由组网部门分配和管理。

2. 域名地址和 IP 地址的映射

域名只是为用户提供了一种方便记忆的手段，主机之间不能直接使用域名进行通信，仍要使用 IP 地址来完成数据的传输。域名到 IP 地址的变换由分布式网络系统 DNS 服务器

来实现。一般子网中都有一个域名服务器，该服务器管理本地子网所连接的主机，也为外来的访问提供 DNS 服务。这种服务采用典型的客户机/服务器访问方式：客户机程序把主机名字发送给服务器，服务器返回对应的 IP 地址。有时被询问的服务器不包含查询的主机记录，根据 DNS 协议，服务器会提供进一步查询的信息，也许是包括相近信息的另外一台 DNS 服务器的地址。

5.2.10.2 远程登录

远程登录(Telnet)是 ARPANET 最早的网络协议之一，今天仍然有广泛的应用。该协议提供了访问远程主机的功能，使本地用户可以通过 TCP 连接登录到远程主机，像使用本地主机一样使用远程主机的资源。在本地终端与远程主机具有异构性时，也不影响它们之间的相互操作。

终端与主机之间的异构性表现在对键盘字符的解释不同。例如，PC 键盘与 IBM 大型机的键盘可能相差很大，使用不同的回车换行符、不同的中断键等。为了使异构性的机器之间能够互操作，Telnet 定义了网络虚拟终端(NVT)。NVT 代码包括标准的 7 位 ASCII 字符集和 Telnet 命令集，这些字符和命令提供了本地终端和远程主机之间的网络接口。

Telnet 采用客户机/服务器工作方式。用户终端运行 Telnet 客户机程序，远程主机运行 Telnet 服务器程序。客户机与服务器程序之间执行 Telnet NVT 协议，而在两端则分别执行各自的操作系统功能。

Telnet 提供一种机制，允许客户机程序和服务器程序协商双方都能接受的操作选项，并提供一组标准选项用于迅速建立需要的 TCP 连接。另外，Telnet 对称地对待连接的两端，并不是专门固定一端为客户端，另一端为服务器端，而是允许连接的任一端与客户机程序相连，另一端与服务器程序相连。

Telnet 服务器可以应付多个并发的连接。通常，Telnet 服务进程等待新的连接，并为每一个连接请求产生一个新的进程。当远程终端用户调用 Telnet 服务时，终端机器上就产生一个客户程序，客户程序与服务器的固定端口(23)建立 TCP 连接，实现 Telnet 服务。客户程序接收用户终端的键盘输入，并发送给服务器；同时服务器送回字符，通过客户机软件的转换显示在用户终端上。用户就是通过这样的方式来发送 Telnet 命令，进而调用服务器主机的资源完成计算任务的。

5.2.10.3 文件传输协议

文件传输协议(FTP)是 Internet 最早的应用层协议。该协议用于主机间传送文件，主机类型可以相同，也可以不同，还可以传送不同类型的文件，如二进制文件或文本文件等。

FTP 采用客户机/服务器工作方式。客户机与服务器之间建立两条 TCP 连接：一条用于传送控制信息，另一条用于传送文件内容。FTP 的控制连接使用 Telnet 协议，主要是利用 Telnet 提供的简单的身份认证系统，供远程系统鉴别 FTP 用户的合法性。

FTP 服务器软件的具体实现依赖于操作系统。一般情况是在服务器一侧运行后台进程 S，等待出现在 FTP 专用端口(21)上的连接请求。当某个客户机向这个专用端口请求建立连接时，进程 S 便激活一个新的 FTP 控制进程 N，处理进来的连接请求。然后 S 进程返回，等待其他客户机访问。进程 N 通过控制连接与客户机进行通信，要求客户在进行文件传送之前输入登录标识符和口令字。如果登录成功，用户可以通过控制连接列出远程目录，设置传送方式，并指明要传送的文件名。当用户获准按照所要求的方式传送文件之后，进程 N

激活另一个辅助进程 D 来处理数据传送。D 进程主动开通第二条数据连接(端口号为 20)，并在文件传送完成后立即关闭此连接，D 进程也自动结束。如果用户还要传送另一个文件，再通过控制连接与 N 进程会话，请求另一次传送。

FTP 是一种功能很强的协议，除了从服务器向客户机传送文件之外，还可以进行第三方传送，这时客户机必须分别开通同两个主机(比如 A 和 B)之间的控制连接。如果客户机获准从 A 机传出文件和向 B 机传入文件，则 A 服务器程序就建立一条到 B 服务器程序的数据连接。客户机保持文件传送的控制权，但不参与数据传送。

FTP 提供的命令十分丰富，包括文件传送、文件管理、目录管理、连接管理等一般文件系统具有的操作功能，还可以用 help 命令查阅各种命令的使用方法。

5.2.10.4　电子邮件

在众多的网络应用中，电子邮件系统是应用最广泛、最有发展前途的网络应用之一。电子邮件系统是基于客户机/服务器方式，客户端也叫作用户代理(User Agent)，提供用户界面，负责邮件发送的准备工作；服务器端也叫作传输代理(Message Transfer Agent)，负责邮件的传输，它采用端到端的传输方式。

电子邮件的内容大多为文本格式，也可以是图形或二进制文件(程序、数据库、字处理文件)，这些特殊数据在传送之前必须转换成相应的文本信息。目前，电子邮件还可以传送照片、声音和视频动画。电子邮件采用存储与转发技术。存储是指发送方将信息存入存储系统。当接收方准备好以后，信息就可以转发过去。邮件的发送方式可以是个人到个人、PC 到 PC 以及程序到程序等各种形式。

在电子邮件发送之前，每个用户必须有一个电子邮箱来存放邮件。每个电子邮箱有一个唯一的邮件地址，当用户发送邮件时，应使用电子邮件地址来说明接收方。一种广泛使用的电子邮箱的格式是：mailbox@computer。这里，mailbox 是一个指明用户邮箱的字符串，而 computer 是一个指明邮箱所在的计算机的字符串，即域名。

广泛使用的电子邮件协议是简单邮件传输协议(Simple Mail Transfer Protocol，SMTP)。当邮件传输程序与远程服务器通信时，它构造一个 TCP 连接，并在此上面进行通信。一旦连接建立，这两个程序就遵循 SMTP 协议，它允许发送方指定接收方以及传输电子邮件信息。SMTP 使用的 TCP 端口号为 25。

TCP/IP 协议簇包含一个提供对电子邮件邮箱进行远程存取的协议，称为邮局协议(POP)。电子邮箱放在一台运行 POP 协议的服务器上，服务器的客户可实现对邮箱的邮件存取。POP 协议对于拨号连接的用户特别适用，用户只需与邮箱所在的计算机建立一个拨号连接，就可以与服务器进行通信，收发电子邮件。

5.2.10.5　WWW 和超文本传输协议

1. WWW 的工作原理

WWW 是基于客户机/服务器模式的应用系统。WWW 服务器负责对各种信息进行组织，WWW 客户机(浏览器)负责如何显示信息和向服务器发送请求。客户端和服务器之间的传输协议采用的是超文本传输协议(HTTP)，服务器端软件通常称为 WWW 服务器，客户端软件通常称为浏览器。

2. URL

在 Web 上寻找信息的关键在于了解 Web 服务器和客户端如何定位服务器和文件的位置。Web 使用统一资源定位器(URL)来标识 Web 页和其他资源。

下面是一个 URL 示例。

http://www.w3c.org/Protocols/index.html

它可以分为以下几部分。

- Protocol://(协议)。
- Servername.domain(服务器名.域)。
- directory/(目录)。
- file(文件)。

在上述示例中：协议是 http；全称域命名为 www.w3c.org；目录名为 Protocols；文件为 index.html。

其他常见的 URL 如下。

- ftp://服务器域名/目录/文件。
- ftp://用户名@服务器域名/目录/文件。
- telnet://服务器域名。
- news://新闻服务器域名/新闻组。

以上 URL 分别表示通过匿名 FTP 请求文档、使用用户名访问 FTP 请求文档、使用 Telnet 访问服务器、请求访问 usenet 新闻组等。

3. 超文本传输协议

超文本传输协议(HTTP)采用了客户机/服务器模式，在服务器与客户机之间建立一条 TCP 连接。默认情况下，服务器使用熟知端口 80，而客户机使用短暂端口。

HTTP 是一种面向事务的应用层协议，每一事务的处理是独立的。通常情况下，HTTP 会为每一事务创建一个客户机与服务器间的 TCP 连接，一旦事务处理结束，HTTP 就切断客户机与服务器间的连接，若客户取下一个文件时，还要重新建立连接。

HTTP 将一次请求/服务的全过程定义为一个简单事务处理，它由以下 4 个步骤组成。

(1) 客户机与服务器建立连接。

(2) 客户向服务器提出请求，在请求中指明欲操作的页。

(3) 如果请求被接受，服务器送回应答。

(4) 客户机与服务器断开连接。

HTTP 报文有以下两种：请求报文和响应报文。它们都由 3 个部分组成：开始行(用于区分是请求报文还是响应报文)、首部行(说明浏览器、服务器或报文主体的一些信息)和实体主体(报文中的内容)。

4. HTML

HTML(超文本标记语言)是制作网页的语言。HTML 中的命令叫作“标记(Tag)”，标记的语法格式如下。

```
<tag>信息</tag>
```

例如<HEAD>和</HEAD>分别表示网页头部的开始和结束，而<BODY>和</BODY>则分别表示网页主体的开始和结束。



5.3 真题详解

试题 1 （2017 年下半年试题 19）

以下关于 OSPF 路由协议的描述中，错误的是 (19) 。

(19) A. 采用 Dijkstra 算法计算到达各个目标的最短通路
B. 计算并得出整个网络的拓扑视图
C. 向整个网络中每一个路由器发送链路代价信息
D. 定期向邻居发送 KeepAlive 报文表明存在

参考答案：(19)C。

要点解析：OSPF 基本上仍是一种链路状态协议，OSPF 的路由器维护一个本地链路状态表，并随时向其他邻居的路由发送关于链路状态的更新信息，并不是向网络中每一个路由器发送。

试题 2 （2017 年下半年试题 20）

相比于 TCP，UDP 的优势为 (20) 。

(20) A. 可靠传输　B. 开销较小　C. 拥塞控制　D. 流量控制

参考答案：(20)B。

要点解析：UDP 是无连接不可靠的传输，其优势为简单，效率高，开销小。

试题 3 （2017 年下半年试题 21）

以太网可以传送最大的 TCP 段为 (21) 字节。

(21) A. 1480　B. 1500　C. 1518　D. 2000

参考答案：(21)A。

要点解析：以太网帧数据部分长度最大为 1500B，上层 IP 头部至少 20B，因此传输层最大为 1480B。

试题 4 （2017 年下半年试题 22）

IP 数据报经过 MTU 较小的网络时需要分片。假设一个大小为 1500 字节的报文分为 2 个较小报文，其中一个报文大小为 800 字节，则另一个报文的大小至少为 (22) 字节。

(22) A. 700　B. 720　C. 740　D. 800

参考答案：(22)B。

要点解析：报文大小为 800 字节，至少有 20 字节的首部，则数据部分为 800−20=780(字节)，另一个报文的数据部分(1500−20)−780=700，再加上 20 字节的首部，其大小为 720 字节。实际上各分片的报文要为 8b 的整数倍。

试题 5 （2017 年下半年试题 23）

IPv4 首部中填充字段的作用是 (23) 。

(23) A. 维持最小帧长　B. 保持 IP 报文的长度为字节的倍数
C. 确保首部为 32 比特的倍数　D. 受 MTU 的限制

参考答案：(23)C。

要点解析：IPv4 首部基本单位为 4 字节，在使用可选字段时，必须用填充字段使之成为 4 字节。

试题 6 (2017 年下半年试题 24)

主机甲向主机乙发送了一个 TCP 连接建立请求，主机乙给主机甲的响应报文中，标志字段正确的是__(24)__。

(24) A. SYN=1，ACK=1，FIN=0　　B. SYN=1，ACK=1，FIN=1
C. SYN=0，ACK=1，FIN=0　　D. SYN=1，ACK=0，FIN=0

参考答案：(24)A。

要点解析：TCP 三次握手中，对 TCP 链接请求的响应应答为 SYN=1，ACK=1，FIN=0(代表终止 TCP 链接)。

试题 7 (2017 年下半年试题 25)

浏览器向 Web 服务器发送了一个报文，其 TCP 段不可能出现的端口组合是__(25)__。

(25) A. 源端口号为 2345，目的端口号为 80
B. 源端口号为 80，目的端口号为 2345
C. 源端口号为 3146，目的端口号为 8080
D. 源端口号为 6553，目的端口号为 5534

参考答案：(25)B。

要点解析：向 Web 服务器发送请求时，目标端口是 80 或者是服务器指定的其他端口，源端口通常是一个临时端口，不可能是 1024 以内的端口。

试题 8 (2017 年下半年试题 27)

RSVP 协议通过__(27)__来预留资源。

(27) A. 发送方请求路由器　　B. 接收方请求路由器
C. 发送方请求接收方　　D. 接收方请求发送方

参考答案：(27)B。

要点解析：资源预留的过程从应用程序流的源节点发送 Path 消息开始，该消息沿着流所经路径传到流的目的节点，并沿途建立路径状态；目的节点收到该 Path 消息后，向源节点回复 Resv 消息，并沿途建立预留状态，如果源节点成功接收到预期的 Resv 消息，则认为在整条路径上资源预留成功。

试题 9 (2017 年下半年试题 28)

在 BGP4 协议中，当接收到对方 open 报文后，路由器采用__(28)__报文响应，从而建立两个路由器之间的邻居关系。

(28) A. hello　　B. update　　C. keepalive　　D. notification

参考答案：(28)C。

要点解析：BGP 中，接收到对方 open 报文后，若有错则发出 notification。若能建立连接则发出 keepalive，用来确认 open 报文和周期性地证实邻站关系。

试题 10 (2017 年下半年试题 29 和试题 30)

某网络拓扑如图 5.5 所示。

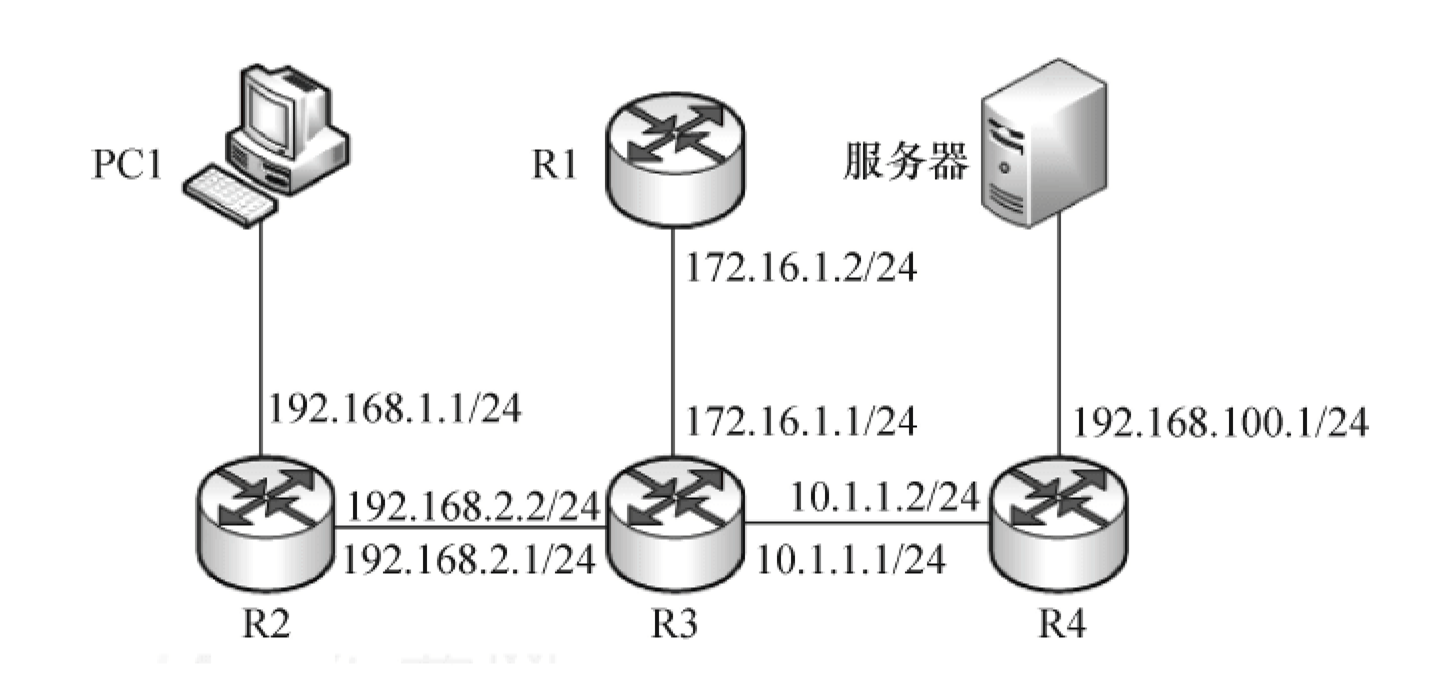


图 5.5　网络拓扑

要得到如下所示的输出信息，应在设备__(29)__上执行__(30)__命令。

IP ADDRESS	MAC ADDRESS	EXPIRE(M)	TYPE	INTERFACE	VPN-INSTANCE VLAN/CEVLAN PVC
10.1.1.2	00e0-fc37-4bc7		I-	GE/0/0	
10.1.1.1	00e0-fcf6-04d5	20	D-0	GE/0/0	
192.168.100.1	00e0-fc37-4bc8		I-	GE/0/1	
192.168.100.100	5489-98b1-211c	17	D-0	GE/0/1	
Total:4	Dynamic:2	Static:0	Interface:2		

(29) A. R1　　B. R2　　C. R3　　D. R4

(30) A. display arp　　B. display rip 1 route

C. display ip routing-table　　D. display MAC

参考答案：(29)D；(30)A。

要点解析：由图可知是一个路由器的 ARP 表，根据四个 IP 地址对应的 MAC 地址可以看到应在 R4 上执行命令，命令是 display arp。

试题 11　(2017 年下半年试题 38)

下面的应用中，__(38)__基于 UDP 协议。

(38) A. HTTP　　B. Telnet　　C. DHS　　D. FTP

参考答案：(38)C。

要点解析：HTTP、FTP、Telnet 都是基于 TCP 协议的。

试题 12　(2017 年下半年试题 39)

在一台服务器上只开放 25 和 110 两个端口，这台服务器可以提供__(39)__服务。

(39) A. E-Mail　　B. Web　　C. DNS　　D. FTP

参考答案：(39)A。

要点解析：端口 25 是 SMTP 协议，110 是 POP3 协议，一个是发邮件协议，另一个是读取邮件的协议，因此这是一台邮件服务器。

试题 13　(2017 年下半年试题 40 和试题 41)

与 HTTP 相比，HTTPS 协议将传输的内容进行加密，更加安全。 HTTPS 基于__(40)__安全协议，其默认端口是__(41)__。

(40) A. RSA　　B. DES　　C. SSL　　D. SSH

(41) A. 1023　　B. 443　　C.80　　D. 8080

参考答案：(40)C；(41)B。

要点解析：HTTPS 是基于 SSL 协议实现的安全传输协议，其标准端口是 443。

试题 14 (2017 年下半年试题 48、49 和试题 50)

某单位网络拓扑如图 5.12 所示。

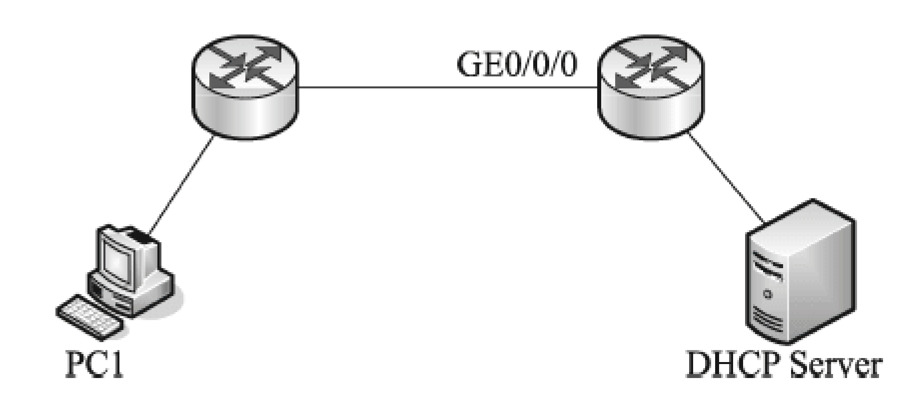


图 5.12　网络拓扑

路由器 AR2 路由表内容如下所示。从路由信息中可以看出，DHCP Server 所在网段是__(48)__；PCL 所在网段是__(49)__；路由器 AR2 接口 GE0/0/0 地址为__(50)__。

```
Route Flags:R - relay,D - download to fib
------------------------------------------
Routing Tables:Public
            Destinations:11     Routes:11
Destination/Mask    Proto  Pre Cost      Flags NextHop        Interface
        127.0.0.0/8    Direct 0    0            D   127.0.0.1       InLoopBack0
        127.0.0.1/32   Direct 0    0            D   127.0.0.1       InLoopBack0
127.255.255.255/32     Direct 0    0            D   127.0.0.1       InLoopBack0
     192.168.0.0/24    RIP   100   1            D   201.1.1.1       GigabitEthernet0/0/0
     192.168.1.0/24    Direct 0    0            D   192.168.1.254   GigabitEthernet0/0/1
   192.168.1.254/32    Direct 0    0            D   127.0.0.1       GigabitEthernet0/0/1
   192.168.1.255/32    Direct 0    0            D   127.0.0.1       GigabitEthernet0/0/1
       201.1.1.0/30    Direct 0    0            D   201.1.1.2       GigabitEthernet0/0/0
       201.1.1.2/32    Direct 0    0            D   127.0.0.1       GigabitEthernet0/0/0
       201.1.1.3/32    Direct 0    0            D   127.0.0.1       GigabitEthernet0/0/0
255.255.255.255/32     Direct 0    0            D   127.0.0.1       InLoopBack0
```

(48) A. 192.168.0.0/24　　B. 192.168.1.0/24
C. 201.1.1.0/30　　D. 127.0.0.0/24

(49) A. 192.168.0.0/24　　B. 192.168.1.0/24
C. 201.1.1.0/30　　D. 127.0.0.0/24

(50) A. 192.168.0.1　　B. 192.168.1.254
C. 201.1.1.1　　D. 201.1.1.2

参考答案：(48)B；(49)A；(50)D。

要点解析：由其路由表可知，192.168.0.0/24 是通过 RIP 学习到的，跳数为 1，下一跳 IP 地址为：201.1.1.1，因此 192.168.0.0 网段符合 PC1 的情况。直连网段有 201.1.1.0/32，192.168.1.0/24，并且 201.1.1.2 是自己的地址，从而可知答案。

试题 15 (2017 年下半年试题 51)

IPv4 的 D 类地址是组播地址，224.0.0.1 表示__(51)__构成的组播组。

(51) A. DHCP 服务器　　B. RIPv2 路由器
C. 本地子网中的所有主机　　D. OSPF 路由器

参考答案：(51)C。

要点解析：多播地址中保留了部分地址，用于特殊的用途。如 224.0.0.1 表示本地子网



的所有主机，224.0.0.2 表示所有路由器。

试题 16　(2017 年下半年试题 52)

在设置家用无线路由器时，下面__(52)__可以作为 DHCP 服务器地址池。

(52) A. 169.254.30.1～169.254.30.254　　B. 224.15.2.1～224.15.2.100
C. 192.168.1.1～192.168. 1.10　　D. 255.15.248.128～255.15.248.255

参考答案：(52)C。

要点解析：DHCP 地址池的地址必须确保在私有地址范围。

试题 17　(2017 年下半年试题 53)

使用 CIDR 技术把 4 个 C 类网络 202.15.145.0/24、202.15.147.0/24、202.15.149.0/24 和 202.15.150.0/24 汇聚成一个超网，得到的地址是__(53)__。

(53) A. 202.15.128.0/20　　B. 202.15.144.0/21
C. 202.15.145.0/23　　D. 202.15.152.0/22

参考答案：(53)B。

要点解析：将四条地址的第三个字段写成二进制位：

1001 0001

1001 0011

1001 0101

1001 0110

经过汇聚后前 21 位相同，故得到的地址为 202.15.144.0/21。

试题 18　(2017 年下半年试题 54)

下面的地址中，可以分配给某台主机接口的地址是__(54)__。

(54) A. 224.0.0.23　　B. 220.168.124.127/30
C. 61.10.191.255/18　　D. 192.114.207.78/27

参考答案：(54)D。

要点解析：224.0.0.23 224 开头表示为组播地址。
220.168.124.127/30 127/30 为广播地址。
61.10.191.255/18 225/18 结尾为广播地址。

试题 19　(2017 年下半年试题 55)

以下 IP 地址中，属于网络 201.110.12.224/28 的主机 IP 是__(55)__。

(55) A. 201.110.12.224　　B. 201.110.12.238
C. 201.110.12.239　　D. 201.110.12.240

参考答案：(55)B。

要点解析：201.110.12.224/28 即 201.110.12.1110 0000，它的可用主机地址范围是：201.110.12.225～201.110.12.238。

试题 20　(2017 年下半年试题 60)

当站点收到“在数据包组装期间生存时间为 0”的 ICMP 报文，说明__(60)__。

(60) A. 回声请求没有得到响应　　B. IP 数据报目的网络不可达

C. 因为拥塞丢弃报文　　D. 因IP数据报部分分片丢失，无法组装

参考答案：(60)B。

要点解析：TTL通常表示包在被丢弃前最多能经过的路由器个数。当计数到0时，路由器决定丢弃该包，并发送一个ICMP报文给最初的发送者。TTL值减为0，说明在网络上经历很多跳之后依旧没有到达目的网络。

试题21　(2017年上半年试题20和试题21)

IPv4首部中首部长度字段(IHL)的值最小为__(20)__。为了防止IP数据报在网络中无限制转发，IPv4首部中通过__(21)__字段加以控制。

(20) A. 2　　B. 5　　C. 10　　D. 15

(21) A. URG　　B. Offset　　C. More　　D. TTL

参考答案：(20)B；(21)D。

要点解析：首部长度占4位，可表示的最大十进制数值为15。因此首部长度的最大值是15个4字节(32位)长的字，即60字节。当IP分组的首部长度不是4字节的整数倍的时候，必须利用最后的填充字段加以填充。典型的IP数据报不使用首部中的选项，因此典型的IP数据报首部长度是20字节。

生存时间字段常用的英文缩写为 TTL。表明数据报在网络中的寿命。由发出数据报的源点设置这个字段。其目的是防止无法交付数据报在因特网上兜圈子，白白消耗网络资源。

试题22　(2017年上半年试题22和试题23)

主机甲向主机乙发送一个TCP报文段，SYN字段为“1”，序列号字段的值为2000，若主机乙同意建立连接，则发送给主机甲的报文段可能为__(22)__；若主机乙不同意建立连接，则__(23)__字段置“1”。

(22) A. (SYN=1，ACK=1，SEQ=2001，ACK=2001)
B. (SYN=1，ACK=0，SEQ=2000，ACK=2000)
C. (SYN=l，ACK=0，SEQ=2001，ACK=2001)
D. (SYN=0，ACK=1，SEQ=2000，ACK=2000)

(23) A. URG　　B. RST　　C. PSH　　D. FIN

参考答案：(22)A；(23)D。

要点解析：主机乙同意建立连接后发回确认包(ACK)应答，即SYN标志位和ACK标志位均为1。同时，将确认序号(Acknowledgement Number)设置为客户的序列号字段的值加1，即2001。

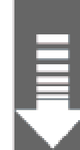
FIN表示连接终止。

试题23　(2017年上半年试题24)

主机甲和主机乙建立一条TCP连接，采用慢启动进行拥塞控制，TCP最大段长度为1000字节。主机甲向主机乙发送第1个段并收到主机乙的确认，确认段中接收窗口大小为3000字节，则此时主机甲可以向主机乙发送的最大字节数是__(24)__字节。

(24) A. 1000　　B. 2000　　C. 3000　　D. 4000

参考答案：(24)B。



要点解析： 慢启动进行拥塞控制算法如下。

MSS 数值：收发双方协商通信时每一个报文段所能承载的最大数据长度。所以 MSS=1000。

慢启动拥塞控制：每当收到一个 ACK，cwnd++，呈线性上升。

每当过了一个 RTT(发送报文到收到确认报文)，则 cwnd 便会急剧上升。

主机甲发送报文段 M1 时，设置发送窗口 cwnd=MSS。主机甲向主机乙发送第一个报文段。

当主机甲收到报文段 K1 确认，则发送窗口 cwnd=cwnd+MSS，即 cwnd=2MSS，主机甲可以向主机乙发送报文段 M2、M3。

当主机甲收到报文段 K2、K3 确认，则发送窗口 cwnd=cwnd+2MSS，即 cwnd=4MSS，当前主机甲可以向主机乙发送报文段 M4、M5、M6、M7。

当主机甲收到报文段 K4、K5、K6、K7 确认，则发送窗口 cwnd=cwnd+4MSS，即 cwnd=8MSS，当前主机甲可以向主机乙发送报文段 M8～M15。

发送方窗口的上限值=Min[rwnd,cwnd]。

因此当主机甲收到第一个报文段确认后，准备发送报文段时，cwnd=2MSS=2000。故主机甲可以发送最大 2000 字节。

试题 24　(2017 年上半年试题 25 和试题 26)

RIPv2 对 RIPv1 协议的改进之一为路由器有选择地将路由表中的信息发送给邻居，而不是发送整个路由表。具体地说，一条路由信息不会被发送给该信息的来源，这种方案称为 __(25)__，其作用是 __(26)__。

(25) A. 反向毒化　　B. 乒乓反弹
C. 水平分割法　　D. 垂直划分法

(26) A. 支持 CIDR　　B. 解决路由环路
C. 扩大最大跳步数　　D. 不使用广播方式更新报文

参考答案： (25)C；(26)B。

要点解析： 水平分割法，从一个方向来的路由信息，不能再放入发回那个方向的路由更新包且又发回那个方向。这是一种能解决路由环路的有效方法。

试题 25　(2017 年上半年试题 27)

OSPF 协议把网络划分成 4 种区域(Area)，其中 __(27)__ 不接受本地自治系统以外的路由信息，对自治系统以外的目标采用默认路由 0.0.0.0。

(27) A. 分支区域　　B. 标准区域　　C. 主干区域　　D. 存根区域

参考答案： (27)D。

要点解析： 如果将区域看成一个节点，则 OSPF 是以主干区域(area0)为顶点，其他区域为终端的星型拓扑结构。

标准区域可以接受链路更新信息和路由总结。

存根区域是不接受自治系统以外的路由信息的区域。如果需要自治系统以外的路由，它使用默认路由 0.0.0.0。

试题 26 (2017 年上半年试题 28、29 和试题 30)

某客户机请求 Web 站点服务的以太网数据帧(前 160 字节)如下图所示，则客户机默认网关的物理地址为__(28)__。客户机在查找默认网关的物理地址时使用的协议是__(29)__，发出的数据帧中目的 MAC 地址为__(30)__。

```
0000  00 23 89 1a 06 7c 00 1d 7d 39 62 3e 08 00 45 00   . #. . . |. .   }9b>. . E. .
0010  01 3b 36 43 40 00 40 06 17 d1 db f5 43 de 7b 7d   . ;6c@. @. . . . . . C. . {}
0020  50 58 06 55 00 50 34 94 05 db b7 cf 20 28 50 18   PX. U. P4.   . . . .   (P.
0030  ff ff ec d6 00 00 47 45 54 20 2f 71 2e 68 74 6d   . . . . . . . GE  T /q. htm
0040  6c 3f 6e 61 6d 65 3d 45 78 74 53 6d 61 72 74 77   l?name=E  xtSmartw
0050  69 7a 49 45 26 73 65 76 65 72 3d 36 2e 30 2e 32   izIE&sev  er=6. 0. 2
0060  39 30 30 2e 32 31 38 30 26 61 70 70 76 65 72 3d   900. 2180  &appver=
0070  31 2e 30 2e 30 2e 31 30 30 37 26 6d 69 64 34 61   1. 0. 0. 10  07&mid=d
0080  30 38 63 37 39 33 30 34 35 36 63 61 30 66 34 61   08c79304  56ca0f4a
0090  34 39 33 32 36 33 63 32 37 36 35 62 37 34 32 26   493263c2  765b742&
```

(28) A. 00-23-89-1a-06-7c　　B. 00-1d-7d-39-62-3e
C. 00-00-00-00-00-00　　D. ff-ff-ff-ff-ff

(29) A. FTP　　B. ARP　　C. BGP　　D. ICMP

(30) A. 00-23-89-1a-06-7c　　B. 00-ld-7d-39-62-3e
C. 00-00-00-00-00-00　　D. ff-ff-ff-ff-ff

参考答案：(28)A；(29)B；(30)D。

要点解析：默认网关参考第一条记录，后面的是网关的物理地址。ARP 协议的功能是通过目标主机的 IP 抵制，查询目标之间的 MAC 地址，实现 IP 地址与 MAC 地址的映射，从而保证通信的顺利进行。

试题 27 (2017 年上半年试题 51)

DHCP 服务器给 PC1 分配 IP 地址时默认网关地址是 202.117.110.65/27，则 PC1 的地址可能是__(51)__。

(51) A. 202.117.110.94　　B. 202.117.110.95
C. 202.117.110.96　　D. 202.117.110.97

参考答案：(51)A。

要点解析：202.117.110.65/27 说明本地址块的可用地址是 202.117.110.65～202.117.110.94。

试题 28 (2017 年上半年试题 52)

某单位 IP 地址需求数如表 5.5 所示，给定地址 192.168.1.0/24，按照可变长子网掩码的设计思想，部门 3 的子网掩码为__(52)__。

表 5.5　某单位 IP 地址需求数

二级单位名称	IP 地址需求数
部门 1	100
部门 2	50
部门 3	30
部门 4	10
部门 5	10

(52) A. 255.255.255.128　　B. 255.255.255.192
C. 255.255.255.224　　D. 255.255.255.240

参考答案：(52)C。





要点解析： 首先 192.168.1.0/24 分成两个子网，一个给部门 1 用，另外一个继续划分为两个子网，一个给部门 2 用，另一个继续划分子网，一个给部门 3 用，剩下的依旧划分子网，给部门 4、5 用。因此部门 3 的子网掩码是 255.255.255.224。

试题 29　(2017 年上半年试题 53 和试题 54)

假设某单位有 1000 台主机，则至少需分配__(53)__个 C 类网络，若分配的超网号为 202.25.64.0，则地址掩码是__(54)__。

(53) A. 4　　B. 8　　C. 12　　D. 16

(54) A. 255.255.224.0　　B. 255.255.240.0
　　C. 255.255.248.0　　D. 255.255.252.0

参考答案： (53)A；(54)D。

要点解析： 一个 C 类网络 254 台主机，1000 台主机需要 4 个 C 类网络。容纳这 1000 台主机的超网掩码是 255.255.252.0。

试题 30　(2017 年上半年试题 55)

在网络 101.113.10.0/29 中，能接收到目的地址是 101.113.10.7 的报文的主机数最多有__(55)__个。

(55) A. 1　　B. 3　　C. 5　　D. 6

参考答案： (55)D。

要点解析： 网络 101.113.10.0/29 中，可用主机范围是 101.113.10.1～101.113.10.6，主机数是 6。

试题 31　(2016 年下半年试题 13)

TCP/IP 网络中的__(13)__实现应答、排序和流控功能。

(13) A. 数据链路层　　B. 网络层　　C. 传输层　　D. 应用层

参考答案： (13)C。

要点解析： 传输层提供应用程序间的通信，包括格式化信息流，提供可靠传输。

试题 32　(2016 年下半年试题 20)

下面哪个协议可通过主机的逻辑地址查找对应的物理地址？__(20)__

(20) A. DHCP　　B. SMTP　　C. SNMP　　D. ARP

参考答案： (20)D。

要点解析： ARP 地址解析协议的功能是通过目标主机的 IP 地址，查询目标主机的 MAC 地址，实现了 IP 地址与 MAC 地址的映射，保证通信的顺利进行。

试题 33　(2016 年下半年试题 21)

下面的应用层协议中通过 UDP 传送的是__(21)__。

(21) A. SMTP　　B. TFTP　　C. POP3　　D. HTTP

参考答案： (21)B。

要点解析： TFTP 是简单文件传输协议，传输层的承载协议是 UDP。

试题 34　(2016 年下半年试题 22)

代理 ARP 是指__(22)__。

(22) A. 由邻居交换机把 ARP 请求传送给远端目标
B. 由一个路由器代替远端目标回答 ARP 请求
C. 由 DNS 服务器代替远端目标回答 ARP 请求
D. 由 DHCP 服务器分配一个回答 ARP 请求的路由器

参考答案：(22)B。

要点解析：路由器从开启 ARP 代理的接口收到一个 ARP 请求，并且该目标 IP 地址是可达的，而且这个对应的路由条目的出接口不是收到该 ARP 请求的接口，那么路由器就将执行代理 ARP 功能。

试题 35 (2016 年下半年试题 23)

如果路由器收到了多个路由协议转发的、关于某个目标的多条路由，它如何决定采用哪个路由？ (23) 。

(23) A. 选择与自己路由协议相同的　　B. 选择路由费用最小的
C. 比较各个路由的管理距离　　D. 比较各个路由协议的版本

参考答案：(23)C。

要点解析：管理距离(AD)是各种路由协议的优先权，当收到了多个路由协议转发的，关于某个目标的多条路由，比较不同协议到达目的网络的 AD 值，值越小表明这条路由可信度级别越高，被采用的机会也越大。路由费用是一种路由协议对于到达目标网络的各种可能路径的成本衡量，比如 RIP 协议中的 hops。

试题 36 (2016 年下半年试题 24)

下面的选项中属于链路路由选择协议的是 (24) 。

(24) A. OSPE　　B. IGRP　　C. BGP　　D. RIPv2

参考答案：(24)A。

要点解析：IGRP、BGP、RIPv2 是距离矢量路由协议。运行链路状态路由协议的路由器，在相互学习路由之间，会首先想自己的邻居路由学习整个网络的拓扑结构，并在自己的内存中建立一个拓扑表，然后使用最短路径优先 SPF 算法，从自己的拓扑表中计算出路由来，OSPF 协议就是一个典型的链路路由选择协议。

试题 37 (2016 年下半年试题 25 和试题 26)

图 5.7 所示的 OSPE 网络由多个区域组成。在这些路由器中，属于主干路由器的是 (25) ，属于自治系统边界路由器(ASBR)的是 (26) 。

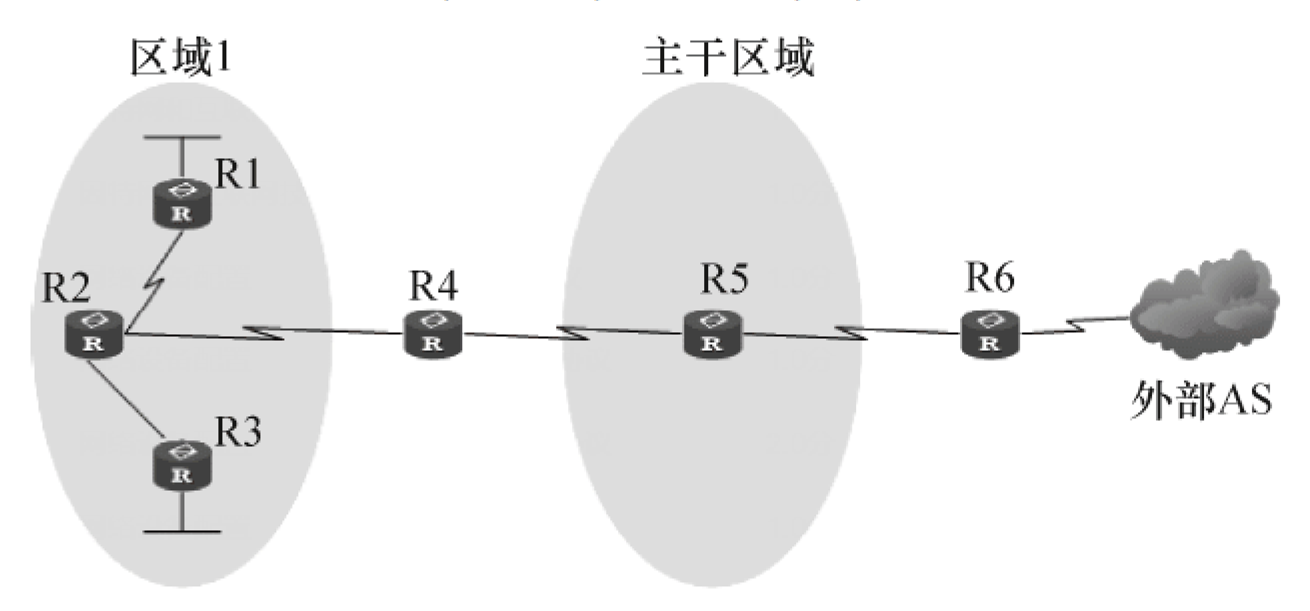
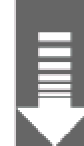


图 5.7 OSPE 网络组成



(25) A. R1　　B. R2　　C. R3　　D. R4
(26) A. R3　　B. R4　　C. R5　　D. R6

参考答案：(25)D；(26)D。

要点解析：主干路由器是指至少有一个接口定义为主干区域的路由器。任何一个和主干区域互连的 ABR 或者 ASBR 也称为主干路由器。AS 边界路由器是和 AS 外部的路由器互相交换路由信息的 OSPF 路由器。该路由器在 AS 内部通告其所得到的 AS 外部路由信息，这样的话 AS 内部所有的路由器都能够知道 AS 边界路由器的路由信息。

试题 38 （2016 年下半年试题 27）

RIPv2 与 RIPv1 相比，它改进了什么？ (27) 。

(27) A. RIPv2 的最大跳数扩大了，可以适应规模更大的网络
B. RIPv2 变成无类别的协议，必须配置子网掩码
C. RIPv2 用跳数和带宽作为度量值，可以有更多的选择
D. RIPv2 可以周期性地发送路由更新，收敛速度比原来的 RIP 快

参考答案：(27)B。

要点解析：RIPv1 和 RIPv2 版本的区别是，RIPv1 是有类别的路由协议，它只支持以广播方式发布协议报文。RIPv1 的协议报文无法携带掩码信息，它只能识别 A、B、C 类标准分类网段的路由，而 RIPv2 是一种无类别路由协议，使用 224.0.0.9 的组播地址，支持 MD5 认证。

试题 39 （2016 年下半年试题 34）

在进行域名解析过程中，当主域名服务器查找不到 IP 地址时，由 (34) 负责域名解析。

(34) A. 本地缓存　　B. 辅助域名服务器
C. 根域名服务器　　D. 转发域名服务器

参考答案：(34)C。

要点解析：主域名服务器：负责维护一个区域的所有域名信息，是特定的所有信息的权威信息源，数据可以修改。

辅助域名服务器：当主域名服务器出现故障、关闭或负载过重时，辅助域名服务器作为主域名服务器的备份提供域名解析服务。辅助域名服务器中的区域文件中的数据是从另外的一台主域名服务器中复制过来的，是不可以修改的。

缓存域名服务器：从某个远程服务器取得每次域名服务器的查询回答，一旦取得一个答案就将它放在高速缓存中，以后查询相同的信息就用高速缓存中的数据回答，缓存域名服务器不是权威的域名服务器，因为它提供的信息都是间接信息。

转发域名服务器：负责所有非本地域名的本地查询。转发域名服务器接到查询请求后，在其缓存中查找，如找不到就将请求依次转发到指定的域名服务器，直到查找到结果为止，否则返回无法映射的结果。

根域名服务器：知道所有顶级域名服务器的域名和 IP 地址，只要本地域名无法解析的话，都首先求助于根域名服务器。

试题40 (2016年下半年试题35)

在建立TCP连接过程中，出现错误连接时，__(35)__标志字段置“1”。

(35) A. SYN　B. RST　C. FIN　D. ACK

参考答案：(35)B。

要点解析：复位RST为1时，说明TCP连接出现严重错误，需要释放连接，重新建立。

TCP的标志字段(6位)：表示各种控制信息。

URG：紧急指针有效。

ACK：应答顺序号有效。

PSH：推进功能有效。

RST：连接复位为初始状态，通常用于连接故障后的恢复。

SYN：对顺序号同步，用于连接的建立。

FIN：数据发送完，连接可以释放。

试题41 (2016年下半年试题36和试题37)

POP3服务器默认使用__(36)__协议的__(37)__端口。

(36) A. UDP　B. TCP　C. SMTP　D. HTTP

(37) A. 21　B. 25　C. 53　D. 110

参考答案：(36)B；(37)D。

要点解析：客户机通过POP3协议接收邮件，POP3传输层基于TCP协议，端口号为110。

试题42 (2016年下半年试题38)

当客户端收到多个DHCP服务器的响应时，客户端会选择__(38)__地址作为自己的IP地址。

(38) A. 最先到达的　B. 最大的

C. 最小的　D. 租期最长的

参考答案：(38)A。

要点解析：当客户端收到多个DHCP服务器的响应时，客户端会选择最先到达的地址作为IP地址。

试题43 (2016年下半年试题51)

ISP分配给某公司的地址块为199.34.76.64/28，则该公司得到的IP地址数是__(51)__。

(51) A. 8　B. 16　C. 32　D. 64

参考答案：(51)B。

要点解析：网络位28位，主机位4位。IP地址数为2^4=16。

试题44 (2016年下半年试题52)

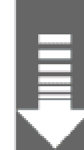
下面是路由表的4个表项，与地址220.112.179.92匹配的表项是__(52)__。

(52) A. 220.112.145.32/22　B. 220.112.145.64/22

C. 220.112.147.64/22　D. 220.112.177.64/22

参考答案：(52)D。

要点解析：将第三、四个字段写成二进制如下。



A：1001 0001.0010 0000

B：1001 0001.0100 0000

C：1001 0011.0100 0000

D：1011 0001.0100 0000

题干中地址的三、四字段：1011 0011.0101 1100，经比较可知匹配的位数最多的是选项 D。

试题 45 （2016 年下半年试题 53）

下面 4 个主机地址中属于网络 110.17.200.0/21 的地址是__(53)__。

(53) A. 110.17.198.0　　　　B. 110.17.206.0

C. 110.17.217.0　　　　D. 110.17.224.0

参考答案：(53)B。

要点解析：110.17.200.0/21=110.107.1100 1000.0。主机号 11 位，其范围为 110.17.11001 000.0～110.17.11001 111.255，四个选项中只有 B 项属于该范围。

试题 46 （2016 年下半年试题 54 和试题 55）

某用户得到的网络地址范围为 110.15.0.0～110.15.7.0，这个地址块可以用__(54)__，其中可以分配__(55)__个可用主机地址。

(54) A. 110.15.0.0/20　　　　B. 110.15.0.0/21

C.110.15.0.0/16　　　　D. 110.15.0.0/24

(55) A. 2048　　B. 2046　　C. 2000　　D. 2056

参考答案：(54)B；(55)B。

要点解析：网络地址块 110.15.0.0～110.15.7.0 可以用 110.15.0.0/21 表示，用于分配 IP 地址的代码占 11 位，除过全 0 的网络地址和全 1 的广播地址外，共有 2046 个主机地址。

试题 47 （2016 年上半年试题 20）

建立组播树是实现组播传输的关键技术，利用组播路由协议生成的组播树是__(20)__。

(20) A. 包含所有路由器的树　　　　B. 包含所有组播源的树

C. 以组播源为根的最小生成树　　　　D. 以组播路由器为根的最小生成树

参考答案：(20)C。

要点解析：多播也可以称为组播，是主机之间一对一的通信模式(UDP)，也就是说加入了同一个组的主机可以接收到此组内的所有数据，网络中的交换机和路由器只向有需求者复制并转发其所需数据。主组播分发树是用于 IP 组播数据包在网络中传输的路径。组播树有两种：源树和共享树。

源树或最短路径树，简称 SPT，源树是以根为组播源的组播分发树。源树的分支形成了通过网络到达接收站点的分布树，因为源树以最短的路径从源路径贯穿网络到达组播接收者，所以又叫最短路径树。

共享分布树，也称为 RP 树或基于核心的树(CBT)。其构造方法为：以网络中某一个指定的路由器为根节点，该路由器称为集合点或中心点，承担转发所有的多播报文的责任。所有要发送组播报文的源主机在发送之前，都需要到 RP 上进行注册，然后通过直连的路由

器来确定到 RP 的最短路径，通过 RP 路由器来确定到目的地的最短路径。

试题 48 (2016 年上半年试题 21)

资源预约协议(RSVP)用在 IETP 定义的集成服务(InsServ)中建立端到端的 QoS 保障机制。下面关于 RSVP 进行资源预约过程的叙述中，正确的是__(21)__。

(21) A. 从目标到源单向预约　　B. 从源到目标单向预约
C. 只适用于点到点的通信环境　　D. 只适用于点到多点的通信环境

参考答案：(21)A。

要点解析：资源预约协议最初是 IETF 为 QoS 的综合服务模型定义的一个信令协议，用于在流(flow)所经路径上为该流进行资源预留，从而满足该流的 QoS 要求。资源预约的过程从应用程序流的源节点发送 Path 消息开始，该消息会沿着流所经路径传到流的目的节点，并沿途建立路径状态；目的节点收到该 Path 消息后，会向源节点回送 Resv 消息，沿途建立预留状态，如果源节点成功收到预期的 Resv 消息，则认为在整条路径上资源预留成功。RSVP 单向的，也就是说从主机 A 到主机 B 的数据流预留的资源，对于从主机 B 到主机 A 的数据流是不起作用的。RSVP 的特征描述如下：①支持单播与组播；②单向预留；③接收者发起预留；④维护 Internet 中的软状态。

试题 49 (2016 年上半年试题 22 和试题 23)

为了解决伴随 RIP 协议的路由环路问题，可以采用水平分割法，这种方法的核心是__(22)__，而反向毒化方法则是__(23)__。

(22) A. 把网络水平地分割为多个网段，网段之间通过指定路由器发布路由信息
B. 一条路由信息不要发送给该信息的来源
C. 把从邻居学习到的路由费用设置为无限大并立即发送给那个邻居
D. 出现路由变化时立即向邻居发送路由更新报文

(23) A. 把网络水平地分割为多个网段，网段之间通过指定路由器发布路由信息
B. 一条路由信息不要发送给该信息的来源
C. 把从邻居学习到的路由费用设置为无限大并立即发送给那个邻居
D. 出现路由器变化时立即向邻居发送路由更新报文

参考答案：(22)B；(23)C。

要点解析：水平分割法的规则和原理是：路由器从某个接口接收到的更新信息不允许再从这个接口发回去。此方法不仅能够阻止路由环路的产生，还能减少路由器更新信息占用的链路带宽资源。反向下毒即保证所有的邻居被下毒，会向毒源的方向反向下毒。

试题 50 (2016 年上半年试题 24)

OSPF 网络被划分为各种区域，其中作为区域之间交换路由信息的是__(24)__。

(24) A. 主干区域　　B. 标准区域　　C. 存根区域　　D. 不完全存根区域

参考答案：(24)A。

要点解析：为了使 OSPF 能用于规模很大的网络，OSPF 将一个自治系统再划分为若干更小的范围，叫作区域。为了使每一个区域能够和本区域以外的区域进行通信，OSPF 使用层次结构的区域划分，在上层的区域叫作主干区域。主干区域的标识符为 0.0.0.0，其作用



是连通其他在下层的区域，从其他区域来的信息都由区域边界路由器进行概括。

试题 51　(2016 年上半年试题 25 和试题 26)

OSPF 将路由器连接的物理网络划分为以下 4 种类型，以太网属于__(25)__，X.25 分组交换网属于__(26)__。

(25) A. 点对点网络　　B. 广播多址网络
C. 点到多点网络　　D. 非广播多址网络

(26) A. 点对点网络　　B. 广播多址网络
C. 点到多点网络　　D. 非广播多址网络

参考答案：(25)B；(26)D。

要点解析：根据路由器所连接的物理网络不同，OSPF 将网络划分为四种类型：广播多路访问型(Broadcast multiAccess)、非广播多路访问型(None Broadcast multiAccess)、点到点型(Point-to-Point)、点到多点型(Point-to-MultiPoint)。其中广播多路访问型网络如 Ethernet、Token Ring、FDDI。NBMA 类型网络如 Frame Relay、X.25、SMD5。Point-to-Point 型网络如 PPP、HDLC。

试题 52　(2016 年上半年试题 27)

采用 DHCP 动态分配 IP 地址，如果某主机开机后没有得到 DHCP 服务器的响应，则该主机获取的 IP 地址属于网络__(27)__。

(27) A. 192.168.1.0/24　　B. 172.16.0.0/24
C. 202.117.0.0/16　　D. 169.254.0.0/16

参考答案：(27)D。

要点解析：四次申请之后，如果仍未能收到服务器的回应，则运行 Windows 的 DHCP 客户机将从 169.254.0.0/16 这个自动保留的私有 IP 地址(APIPA)中选用一个 IP 地址，但运行其他操作系统的 DHCP 客户机将无法获得 IP 地址。

试题 53　(2016 年上半年试题 28、29、30 和试题 31)

某网络拓扑结构如图 5.14 所示。

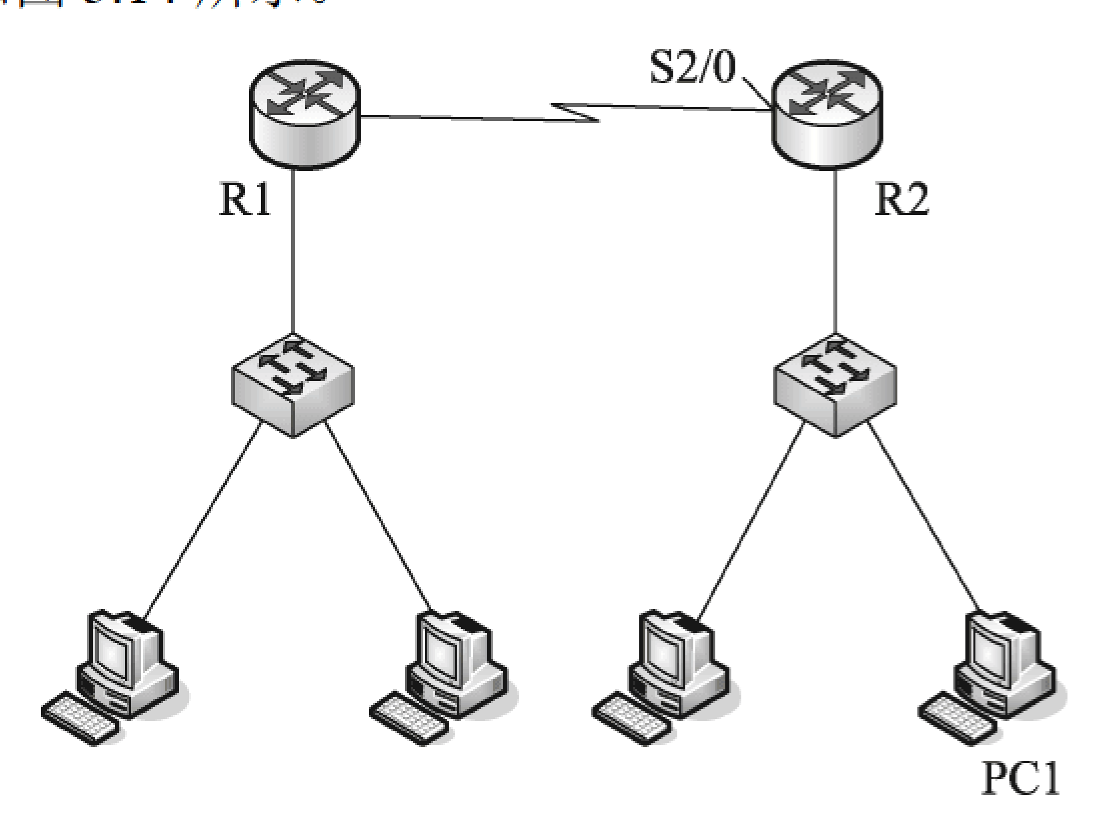


图 5.14　网络拓扑结构

在路由器 R2 上采用命令__(28)__得到如图 5.15 所示结果。PC1 可能的 IP 地址为

(29)，路由器 R2 的 S2/0 口的 IP 地址为(30)。若在 PC1 上查看主机的路由表，采用的命令为(31)。

```
R2>
    ...
    R      192.168.0.0/24[120/1]via 202.117.112.1,00:00:11, Serial2/0
    C      192.168.1.0/24 is directly connected, FastEthernet0/0
               202.117.112.0/30 is subnetted, 1 subnets
    C      202.117.112.0 is directly connected, Serial2/0
R2>
```

图 5.15　命令执行结果

(28) A. nslookup　B. route print　C. IP routing　D. show IP route
(29) A. 192. 168. 0. 1　B. 192. 168. 1. 1
C. 202. 117. 112. 1　D. 202. 117. 112. 2
(30) A. 192. 168. 0. 1　B. 192. 168. 1. 1
C. 202. 117. 112. 1　D. 202. 117. 112. 2
(31) A. nslookup　B. route print　C. IP routing　D. show IP route

参考答案：(28)D；(29)B；(30)D；(31)B。

要点解析：在路由器上显示路由表的命令是：show IP route。

在路由器表中，C 表示直连的路由，R 表示路由器学习到的路由；路由器 R2 直连的局域网段为 192.168.1.0/24，那么 PC1 的地址就属于这一网段，路由器 R2 直连的广域网段是 202.117.112.0/30，那么 S2/0 口就属于这个网段，又因为学习到的 192.168.0.0/24 是通过下一跳也就是 R1 和 R2 相连的接口地址 202.117.112.1，则 S2/0 口的地址可以根据 202.117.112.0/30 和 202.117.112.1 算出为 202.117.112.2。

在主机上查看路由表的命令为 route print 或 netstat –r。

试题 54　(2016 年上半年试题 32、33 和试题 34)

DNS 反向搜索功能的作用是(32)，资源记录 MX 的作用是(33)，DNS 资源记录(34)定义了区域的反向搜索。

(32) A. 定义域名服务器的别名　B. 将 IP 地址解析为域名
C. 定义域邮件服务器地址和优先级　D. 定义区域的授权服务器
(33) A. 定义域名服务器的别名　B. 将 IP 地址解析为域名
C. 定义域邮件服务器地址和优先级　D. 定义区域的授权服务器
(34) A. SOA　B. NS　C. PTR　D. MX

参考答案：(32)B；(33)C；(34)C。

要点解析：DNS 的反向区域负责从 IP 到域名的解析，因此如果要创建 PTR 记录，必须在反向区域中创建。

MX 记录也叫作邮件路由记录，用户可以将该域名下的邮件服务器指向到自己的 Mail Server 上，然后即可自行操控所有的邮箱设置。

PTR 记录也被称为指针记录，PTR 记录是 A 记录的逆向记录，作用是把 IP 地址解析为域名。



试题 55　(2016 年上半年试题 37)

在浏览器的地址栏中输入 xxxyftp. abc. com. cn，该 URL 中__(37)__是要访问的主机名。

(37) A. xxxyftp　　B. abc　　C. com　　D. cn

参考答案：(37)A。

要点解析：在浏览器的地址栏中输入 xxxyftp. abc. com. cn，该 URL 中 xxxyftp 是要访问的主机名，cn 是顶级域名，com 是二级域名，abc 是三级域名。

试题 56　(2016 年上半年试题 38)

下列关于 DHCP 服务的叙述中，正确的是__(38)__。

(38) A. 一台 DHCP 服务器只能为其所在网段的主机分配 IP 地址

B. 对于移动用户设置较长的租约时间

C. DHCP 服务器不需要配置固定的 IP 地址

D. 在 Windows 客户机上可使用 ipconfig/release 释放当前 IP 地址

参考答案：(38)D。

要点解析：DHCP 服务可以跨越子网分配，对移动用户一般设置租约比较短的时间，对固定用户一般设置租约比较长的时间。DHCP 服务器一般配置固定的 IP 地址，在 Windows 客户机上可使用 ipconfig/release 释放当前 IP 地址，使用 ipconfig/renew 重新获取 IP。

试题 57　(2016 年上半年试题 39 和试题 40)

当接收邮件时，客户端与 POP3 服务器之间通过__(39)__建立连接，所使用的端口是__(40)__。

(39) A. UDP　　B. TCP　　C. HTTP　　D. HTTPS

(40) A. 25　　B. 52　　C. 1100　　D. 110

参考答案：(39)B；(40)D。

要点解析：POP3 协议默认端口为 110。

POP3 协议默认传输协议为 TCP。

POP3 协议适用的构架结构为 C/S。

POP3 协议的访问模式为离线访问。

试题 58　(2016 年上半年试题 51)

下面 4 个主机地址中属于网络 220. 115. 200. 0/21 的地址是__(51)__。

(51) A. 220. 115. 198. 0　　B. 220. 115. 206. 0

C. 220. 115. 217. 0　　D. 220. 115. 224. 0

参考答案：(51)B。

要点解析：220. 115. 200. 0/21 表示该地址的网络号有 21 位，主机位占 11 位，那么该地址块的范围是 220.115.11001 000.00000000～220.115.11001 111.11111111(220.115.200.0～220.115.207.255)。

试题 59　(2016 年上半年试题 52 和试题 53)

假设路由表有 4 个表项如下所示，那么与地址 115. 120. 145. 67 匹配的表项是__(52)__。与地址 115.120.179.92 匹配的表项是__(53)__。

(52) A. 115.120.145.32　　B. 115.120.145.64
C. 115.120.147.64　　D. 115.120.177.64

(53) A. 115.120.145.32　　B. 115.120.145.64
C. 115.120.147.64　　D. 115.120.177.64

参考答案：(52)B；(53)D。

要点解析：115.120.145.67 的第三项和第四项展开成二进制形式：115.120.1001 0001.0100 0011。再将四个选项 IP 地址一一展开成二进制形式，寻找最大的相同位数。

A：115.120.1001 0001.0010 0000

B：115.120.1001 0001.0100 0000

C：115.120.1001 0011.0100 0000

D：115.120.1011 0001.0100 0000

显然，匹配度最高的为选项 B。(53)同理。

试题 60　(2016 年上半年试题 54 和试题 55)

假设分配给用户 U1 的网络号为 192. 25. 16. 0～192. 25. 31. 0，则 U1 的地址掩码应该为 (54) ；假设分配给用户 U2 的网络号为 192. 25. 64. 0/20，如果路由器收到一个目标地址为 11000000. 00011001. 01000011. 00100001 的数据报，则该数据报应传送给用户 (55) 。

(54) A. 255.255.255.0　　B. 255.255.250.0
C. 255.255.248.0　　D. 255.255.240.0

(55)A. U1　　B. U2　　C. U1 或 U2　　D. 不可到达

参考答案：(54)D；(55)B。

要点解析：16 个 C 类地址进行聚合 192. 25. 16. 0～192. 25. 31. 0，聚合后最大的相同位数为 20 位，那么 U1 的地址掩码应为 1111 1111.1111 1111.1111 0000.0000 0000，即 255.255.240.0 聚合后的地址为 192.25.16.0/20。分配给用户 U2 的网络号为 192. 25. 64. 0/20，如果路由器收到一个目标地址为 11000000. 00011001. 01000011. 00100001(192.25.67.33)的数据报，很明显该数据包属于 U2 网络，故数据包应传送给用户 U2。

试题 61　(2015 年下半年试题 11)

集线器与网桥的区别是 (11) 。

(11) A. 集线器不能检测发送冲突，而网桥可以检测冲突
B. 集线器是物理层设备，而网桥是数据链路层设备
C. 网桥只有两个端口，而集线器是一种多端口网桥
D. 网桥是物理层设备，而集线器是数据链路层设备

参考答案：(11)B。

要点解析：集线器是物理层设备，可视为一种特殊的中继器，用于扩大网络；网桥是数据链路层设备，用于连接两个局域网网段。确切地讲，网桥工作在 MAC 子层，只要两个网络的 MAC 子层以上的协议相同，都可以用网桥互连。

试题 62　(2015 年下半年试题 14)

关于 ICMP 协议，下面的论述中正确的是 (14) 。

(14) A. 通过 ICMP 可以找到与 MAC 地址对应的 IP 地址

B. 通过 ICMP 可以把全局 IP 地址转换为本地 IP 地址

C. ICMP 用于动态分配 IP 地址

D. ICMP 可传送 IP 通信过程中出现的错误信息

参考答案：(14)D。

要点解析：ICMP(Internet Control Message Protocol)是 TCP/IP 协议簇的一个子协议，属于网络层协议，主要用于在主机与路由器之间传递控制信息，包括报告错误、交换受限控制和状态信息等。当遇到 IP 数据无法访问目标、IP 路由器无法按当前的传输速率转发数据包等情况时，会自动发送 ICMP 消息。

试题 63　(2015 年下半年试题 20 和试题 21)

图 5.16 中主机 A 和主机 B 通过三次握手建立 TCP 连接，图中(1)处的状态是__(20)__，图中(2)处的数字是__(21)__。

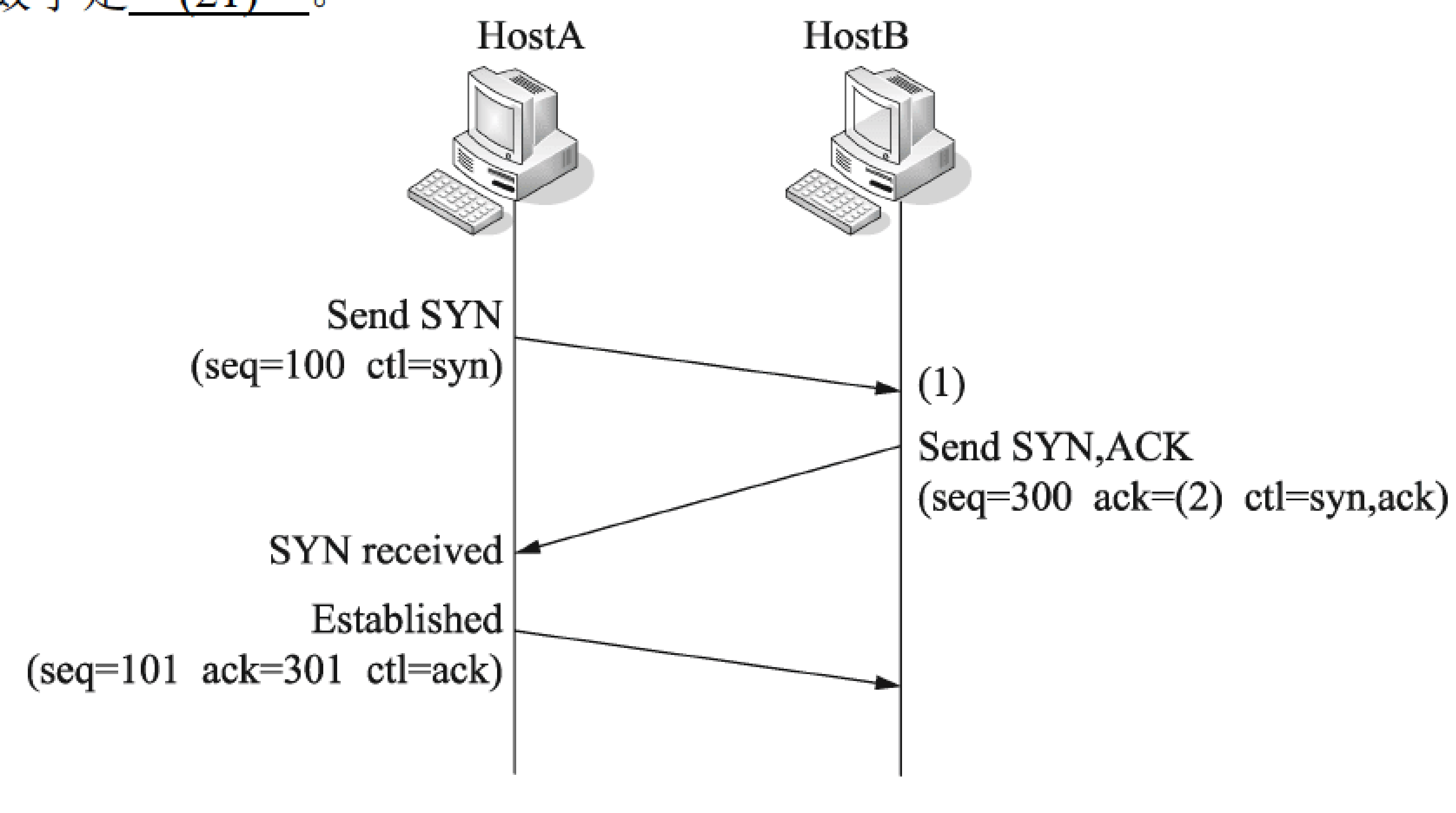


图 5.16　建立 TCP 连接

(20) A. SYN received　　B. Established　　C. Listen　　D. FIN wait

(21) A. 100　　B. 101　　C. 300　　D. 301

参考答案：(20)A；(21)B。

要点解析：TCP 三次握手流程：

(1) A 的 TCP 客户进程首先向 B 发出连接请求报文段，这时首部中的同步位 SYN=1，同时选择一个初始序号 seq=x。TCP 规定，SYN 报文段(SYN=1 的报文段)不能携带数据，但要消耗一个序号。这时候，客户进程进入同步已发送状态。

(2) B 收到这个连接请求之后，如同意建立连接，则向 A 发送确认。在确认报文段中应把 SYN 位和 ACK 位都置 1，确认号是 ack=x+1，同时也为自己选择一个初始序号 seq=y。请注意，这个报文段也不能携带数据，但同样要消耗一个序号。这时 TCP 服务器进程进入同步收到状态。

(3) TCP 客户进程收到 B 的确认后，还要向 B 给出确认，确认报文段的 ACK 置 1，确认号 ack=y+1，则自己的序号 seq=x+1。TCP 协议规定，ACK 报文段可以携带数据，但如果不携带数据则不消耗序号。在这种情况下，下一个数据报文段的序号依然是 seq=x+1。这时，TCP 连接已经建立，A 进入已建立连接状态。

试题 64 (2015 年下半年试题 22)

TCP 使用的流量控制协议是 (22) 。

(22) A. 固定大小的滑动窗口协议　　B. 后退 *N* 帧的 ARQ 协议

C. 可变大小的滑动窗口协议　　D. 停等协议

参考答案：(22)C。

要点解析：TCP 使用一种窗口(window)机制来控制数据流。TCP 的窗口以字节为单位进行调整，以适应接收方的处理能力。处理过程如下。

(1) TCP 连接阶段，双方协商窗口尺寸，同时接收方预留数据缓存区。

(2) 发送方根据协商的结果，发送符合窗口尺寸的数据字节流，并等待对方的确认。

(3) 发送方根据确认信息，改变窗口的尺寸，增加或者减少发送未得到确认的字节流中的字节数。调整过程包括：如果出现发送拥塞，发送窗口缩小为原来的一半，同时将超时重传的时间间隔扩大一倍。

试题 65 (2015 年下半年试题 24、25 和试题 26)

边界网关协议 BGP4 是一种动态路由发现协议，它的主要功能是 (24) 。BGP 路由器之间传送的是 AS 路径信息，这样就解决了 (25) 问题。BGP4 报文封装在 (26) 。

(24) A. 发现新的路由　　B. 计算最短通路

C. 控制路由策略　　D. 维护网络拓扑数据库

(25) A. 路由环路　　B. 最短通路

C. 路由计算　　D. 路由更新

(26) A. IP 数据报　　B. 以太帧

C. TCP 报文　　D. UDP 报文

参考答案：(24)C；(25)A；(26)C。

要点解析：边界网关协议(BGP)是运行于 TCP 上的一种自治系统的路由协议。BGP 的主要目标是为处于不同 AS 中的路由器之间进行路由信息通信提供保障。只是力求寻找一条能够到达目的网络且比较好的路由，而不是要寻找一条最佳路由。BGP 既不是纯粹的矢量距离协议，也不是纯粹的链路状态协议，通常被称为通路向量路由协议。这是因为 BGP 在发布到一个目的网络的可达性的同时，包含了在 IP 分组到达目的网络过程中所必须经过的 AS 的列表。BGP 系统的主要功能是交换其他 BGP 系统的网络可达信息，包括 AS 路径的列表信息，此信息可用于建立 AS 系统连接图，以消除路由环路，以及执行 AS 策略确定。

试题 66 (2015 年下半年试题 27)

在广播网络中，OSPF 协议要选定一个指定路由器(DR)，指定路由器的功能是 (27) 。

(27) A. 发送链路状态公告　　B. 检查网络故障

C. 向其他路由器发送最新路由表　　D. 发现新增加的路由

参考答案：(27)A。

要点解析：为减少网络中的链路状态确认分组 LSA 泛洪传播，OSPF 会在每一个网络中选举一个指定路由器 DR 和一个备用指定路由器 BDR。网络中的路由器都只与 DR、BDR 建立全相邻的邻接关系，其他路由器之间不会建立全相邻的 OSPF 邻接关系。在 OSPF 网络中，各路由器之间不直接两两发链路状态信息，而是通过选举 DR/BDR，以 DR 为主，以



BDR 为备份 DR，把链路状态信息发给 DR/BDR，由 DR 再组播给所有非 DR/BDR 的路由器。

试题 67　(2015 年下半年试题 28 和试题 29)

POP3 协议采用__(28)__模式，客户端代理与 POP3 服务器通过建立__(29)__连接来传送数据。

(28) A. Browser/Server　　B. Client/Server
　　C. Peer to Peer　　D. Peer to Server

(29) A. TCP　　B. UDP　　C. P2P　　D. IP

参考答案：(28)B；(29)A。

要点解析：电子邮件收发过程：发件人调用 PC 中的用户代理撰写和编辑要发送的邮件。发件人的用户代理把邮件用 SMTP 协议发给发送方邮件服务器，SMTP 服务器把邮件临时存放在邮件缓存队列中，等待发送。发送方邮件服务器的 SMTP 客户与接收方邮件服务器的 SMTP 服务器建立 TCP 连接，然后就把邮件缓存队列中的邮件依次发送出去。运行在接收方邮件服务器中的 SMTP 服务器进程收到邮件后，把邮件放入收件人的用户邮箱中，等待收件人进行读取。收件人在打算收信时，就运行 PC 中的用户代理，使用 POP3(或 IMAP)协议读取发送给自己的邮件。请注意，POP3 服务器和 POP3 客户之间的通信是由 POP3 客户发起的。其中 SMTP 和 POP3 协议的传输层的承载协议都是 TCP。

试题 68　(2015 年下半年试题 35)

图 5.17 是 DNS 转发器工作的过程。采用迭代查询算法的是__(35)__。

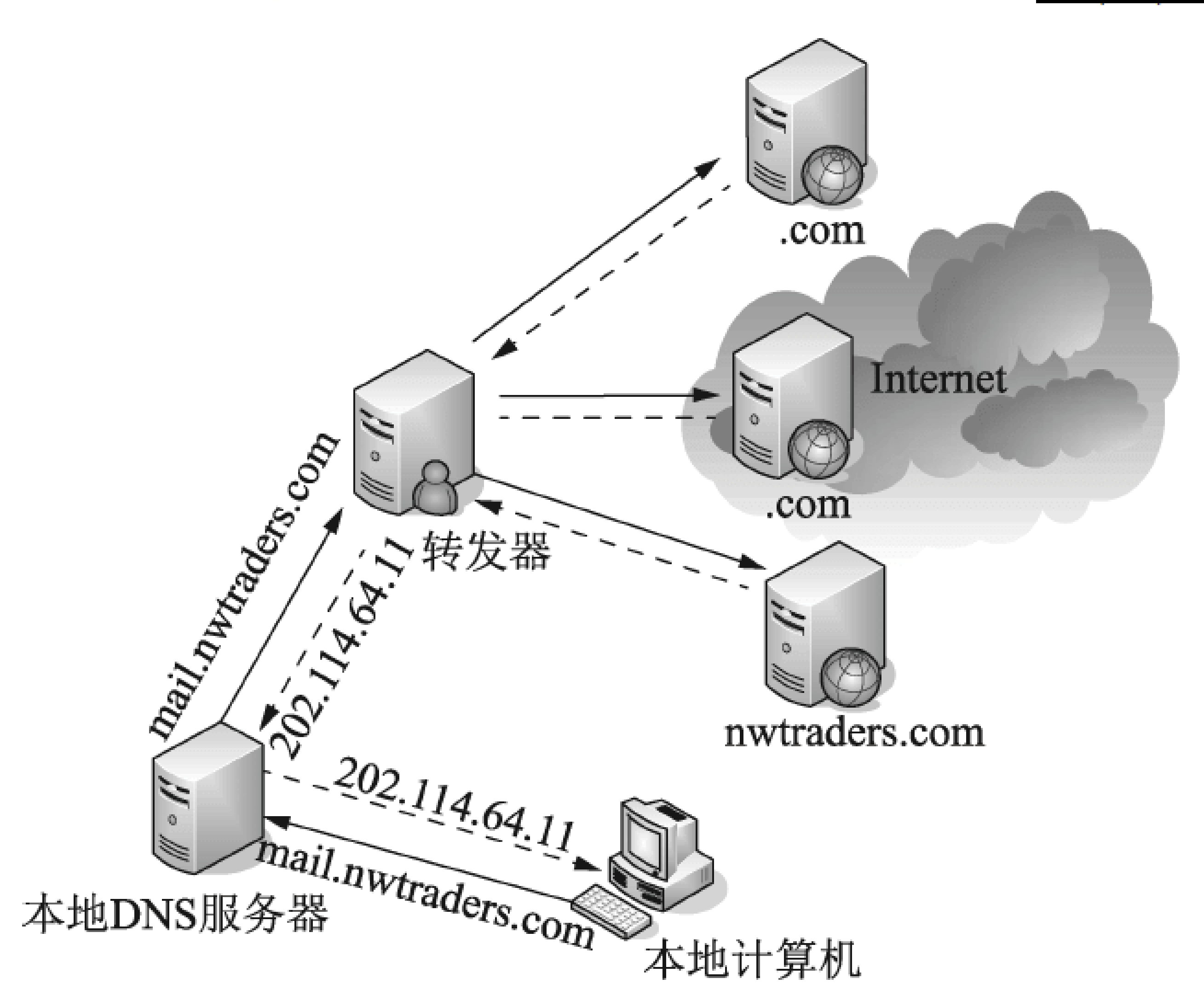


图 5.17　DNS 转发器工作的过程

(35) A. 转发器和本地 DNS 服务器　　B. 根域名服务器和本地 DNS 服务器
　　C. 本地 DNS 服务器和.com 域名服务器　　D. 根域名服务器和.com 域名服务器

参考答案：(35)D。

要点解析：只要发出递归查询，服务器必须回答目标 IP 与域名的映射关系。而迭代查

询是，服务器收到一次迭代查询回复一次结果，这个结果不一定是目标 IP 与域名的映射关系，也可以是其他 DNS 服务器的地址。

一般情况下，从客户端到本地 DNS 服务器是属于递归查询，而 DNS 服务器之间的就是交互查询就是迭代查询。

试题 69 (2015 年下半年试题 36)

下列域名中，格式正确的是__(36)__。

(36) A. -123456.com　　B. 123-456.com
C. 123*456.com　　D. 123456-.com

参考答案：(36)B。

要点解析：域名可以由(a～z、A～Z 大小写等价)26 个英文字母、数字(0～9)以及连接符“-”组成，但是域名的首位和结尾必须是字母或数字。对于域名的长度也有一定的限制。

试题 70 (2015 年下半年试题 37)

以下关于域名查询的叙述中，正确的是__(37)__。

(37) A. 正向查询是检查 A 记录，将 IP 地址解析为主机名
B. 正向查询是检查 PTR 记录，将主机名解析为 IP 地址
C. 反向查询是检查 A 记录，将主机名解析为 IP 地址
D. 反向查询是检查 PTR 记录，将 IP 地址解析为主机名

参考答案：(37)D。

要点解析：DNS 资源记录如下。

① SOA 记录：SOA 说明能解析这个区域的 DNS 服务器中哪个是主服务器。
② NS 记录：用于标识区域的 DNS 服务器有几台提供服务。
③ A 记录：也称为主机记录，是 DNS 名称到 IP 地址的映射，用于正向解析。
④ PTR 记录：IP 地址到 DNS 名称的映射，用于反向解析。

试题 71 (2015 年下半年试题 38)

下列地址中，__(38)__不是 DHCP 服务器分配的 IP 地址。

(38) A. 196.254.109.100　　B. 169.254.109.100
C. 96.254.109.100　　D. 69.254.109.100

参考答案：(38)B。

要点解析：APIPA 是一个 DHCP 故障转移机制。当 DHCP 服务器出故障时，APIPA 在 169.254.0.1 到 169.254.255.254 的私有空间内分配地址，所有设备使用默认的网络掩码 255.255.0.0。

试题 72 (2015 年下半年试题 51)

通过 CIDR 技术，把 4 个主机地址 220.78.169.5、220.78.172.10、220.78.174.15 和 220.78.168.254 组织成一个地址块，则这个超级地址块的地址是__(51)__。

(51) A. 220.78.177.0/21　　B. 220.78.168.0/21
C. 220.78.169.0/20　　D. 220.78.175.0/20

参考答案：(51)B。



要点解析：由于一个 CIDR 地址块中有很多地址，所以在路由表就利用 CIDR 地址块来查询目的网络。这种地址的聚合常称为路由聚合。它可以让路由表中一个项目表示原来传统分类的很多个路由。

把 4 个主机地址 220.78.169.5、220.78.172.10、220.78.174.15 和 220.78.168.254 组织成一个地址块，方法是首先转换为二进制的形式，找出最大的相同位数，作为汇聚后的网络位。由于 220.78 都一样，所以我们只转换第三段。

10101001

10101100

10101110

10101000

所以最大的相同位数是 8+8+5=21。网络地址就是 202.78.168.0/21。

试题 73　(2015 年下半年试题 52)

采用可变长子网掩码可以把大的网络分成小的子网，例如把 A 类网络 60.15.0.0/16 分为两个子网，假设第一个子网为 60.15.0.0/17，则另一个子网为__(52)__。

(52) A. 60.15.1.0/17　　B. 60.15.2.0/17
C. 60.15.100.0/17　　D. 60.15.128.0/17

参考答案：(52)D。

要点解析：把 A 类网络 60.15.0.0/16 分为两个子网，应该拿出 1 位主机位进行子网划分，那么划分的两个子网分别是 60.15.0 0000000 00000000/17 和 60.15.1 0000000 00000000/17。

试题 74　(2015 年下半年试题 53 和试题 54)

假设用户 X 有 4000 台主机，则必须给他分配__(53)__个 C 类网络。如果为其分配的网络号为 196.25.64.0，则给该用户指定的地址掩码为__(54)__。

(53) A. 4　　B. 8　　C. 10　　D. 16

(54) A. 255.255.255.0　　B. 255.255.250.0
C. 255.255.248.0　　D. 255.255.240.0

参考答案：(53)D；(54)D。

要点解析：C 类网络的主机号是 8 位，可容纳 254 台主机，现在用户 X 有 4000 台主机，则必须给他分配的 C 类网络数目为 4000/254=15.7，所以给其分配 16 个 C 类网络。如果为其分配的网络号为 196.25.64.0，给用户指定的地址掩码中 0 的个数，只要保证有 12 个，因为 $2^{12}-2=4096-2=4094$。所以我们选择答案 D，255.255.240.0 子网掩码中 0 的个数是 12 个。

试题 75　(2015 年下半年试题 55 和试题 56)

如果在查找路由表时发现有多个选项匹配，那么应该根据__(55)__原则进行选择。假设路由表有 4 个表项如下所示，那么与地址 139.17.179.92 匹配的表项是__(56)__。

(55) A. 包含匹配　　B. 恰当匹配
C. 最长匹配　　D. 最短匹配

(56) A. 139.17.145.32　　B. 139.17.145 .64
C. 139.17.147.64　　D. 139.17.177.64

参考答案：(55)C；(56)D。

要点解析：最长匹配原则：在使用 CIDR 时，由于采用了网络前缀这种记法，IP 地址由网络前缀和主机号两部分组成，因此在路由表中的项目也要有相应的改变。这时，每个项目由“网络前缀”和“下一跳地址”组成。但是在查找路由表时可能会得到不止一个匹配结果，这样就带来一个问题：我们应当从这些结果中选择哪一条路由呢？

正确的答案是：应当从匹配结果中选择具有最长网络前缀的路由。这叫作最长前缀匹配，这是因为网络前缀越长，其地址块就越小，路由就越具体。

假设路由表有 4 个表项，那么与地址 139.17.179.92 匹配的表项是 139.17.177.64，因为它和 139.17.179.92 具有最多的相同位数。

试题 76 (2015 年下半年试题 67)

多协议标记交换(MPLS)是 IETF 提出的第三层交换标准，以下关于 MPLS 的叙述中，正确的是__(67)__。

(67) A. 带有 MPLS 标记的分组封装在 PPP 帧中传输
B. 传送带有 MPLS 标记的分组之前先要建立对应的网络连接
C. 路由器根据转发目标把多个 IP 流聚合在一起组成转发等价类
D. MPLS 标记在各个子网中是特定分组的唯一标识

参考答案：(67)C。

要点解析：MPLS 是利用标记(label)进行数据转发的。当分组进入网络时，要为其分配固定长度的短的标记，并将标记与分组封装在一起，在整个转发过程中，交换节点仅根据标记进行转发。

有 MPLS 标记的分组不但可以封装在 PPP 帧中传送，还可以封装在以太网、ATM 和帧中继。

MPLS 标记具有局部性，一个标记只是在一定的传输域中有效。

以太网传输数据帧，没有建立连接的概念。

试题 77 (2015 年上半年试题 13)

以下关于网桥和交换机的区别的叙述中，正确的是__(13)__。

(13) A. 交换机主要是基于软件实现，而网桥是基于硬件实现的
B. 交换机定义了广播域，而网桥定义了冲突域
C. 交换机根据 IP 地址转发，而网桥根据 MAC 地址转发
D. 交换机比网桥的端口多，转发速度更快

参考答案：(13)D。

要点解析：网桥用于连接两个局域网，工作在数据链路层。交换机是一种多端口的网桥。网桥可以是专门硬件设备，也可以由计算机加装的网桥软件来实现，这时计算机上会安装多个网络适配器(网卡)。网桥将两个 LAN 连起来，根据 MAC 地址来转发帧，可以看作一个“低层的路由器”。

试题 78 (2015 年上半年试题 16)

当一个帧离开路由器接口时，其第二层封装信息中__(16)__。

(16) A. 数据速率由 10Base-TX 变为 100Base-TX
B. 源和目标 IP 地址改变



C. 源和目标 MAC 地址改变

D. 模拟线路变为数字线路

参考答案：(16)C。

要点解析：广域网的数据链路层协议描述了在系统之间的单一链路上数据帧是如何传送的。为了确保使用恰当的协议，必须在路由器上配置适当的第二层封装。第二层封装中，源和目标 IP 不变，源和目标 MAC 变化。

试题 79　(2015 年上半年试题 17)

以下关于 OSPF 的区域(Area)的叙述中，正确的是__(17)__。

(17) A. 各个 OSPF 区域都要连接到主干区域

B. 分层的 OSPF 网络不需要多个区域

C. 单个 OSPF 网络只有区域 1

D. 区域 ID 的取值范围是 1～32768

参考答案：(17)A。

要点解析：区域 ID 长 32 位，其表示范围为 0～65535。当设置 area 0 时，其区域 ID 为 0.0.0.0。当网络区域为 0 或 0.0.0.0 时称为主干区域。作为主干区域的 area 0 必须存在；所有区域，即使是端区，也必须和骨干区域相连；如果存在多个骨干区域，那么它们必须连续(逻辑上)。

试题 80　(2015 年上半年试题 18)

运行 OSPF 协议的路由器用__(18)__报文来建立和更新它的拓扑数据库。

(18) A. 由其他路由器发送的链路状态公告(LSA)

B. 从点对点链路收到的信标

C. 由指定路由器收到的 TTL 分组

D. 从邻居路由器收到的路由表

参考答案：(18)A。

要点解析：链路状态(LSA)就是 OSPF 接口上的描述信息，例如接口上的 IP 地址、子网掩码、网络类型、Cost 值等，OSPF 路由器之间交换的并不是路由表，而是链路状态(LSA)。OSPF 通过获得网络中所有的链路状态信息，从而计算出到达每个目标精确的网络路径。OSPF 路由器会将自己所有的链路状态毫不保留地全部发给邻居，邻居将收到的链路状态全部放入链路状态数据库(Link-State Database)，邻居再发给自己的所有邻居，并且在传递过程中，绝对不会有任何更改。通过这样的过程，最终，网络中所有的 OSPF 路由器都拥有网络中所有的链路状态，并且所有路由器的链路状态应该能描绘出相同的网络拓扑。

试题 81　(2015 年上半年试题 19)

链路状态路由协议的主要特点是__(19)__。

(19) A. 邻居之间交换路由表　　B. 通过事件触发及时更新路由

C. 周期性更新全部路由表　　D. 无法显示整个网络拓扑结构

参考答案：(19)B。

要点解析：链路状态路由协议只在网络发生变化的时候发送触发式更新(triggered update)，更新是非周期性的。

试题 82 (2015 年上半年试题 21)

运行距离矢量路由协议的路由器__(21)__。

(21) A. 把路由表发送到整个路由域中的所有路由器

B. 使用最短道路算法确定最佳路由

C. 根据邻居发来的信息更新自己的路由表

D. 维护整个网络的拓扑数据库

参考答案：(21)C。

要点解析：距离矢量名称的由来是因为路由是以矢量(距离，方向)的方式被通告出去的，这里的距离是根据度量来决定的。距离矢量协议直接传送各自的路由表信息。网络中的路由器从自己的邻居路由器得到路由信息，并将这些路由信息连同自己的本地路由信息发送给其他邻居，这样一级级地传递下去以达到全网同步。每个路由器都不了解整个网络拓扑，它们只知道与自己直接相连的网络情况，并根据从邻居得到的路由信息更新自己的路由。

试题 83 (2015 年上半年试题 26)

某网络拓扑如图 5.18 所示，若采用 RIP 协议，在路由器 Router2 上需要进行 RIP 声明的网络是__(26)__。

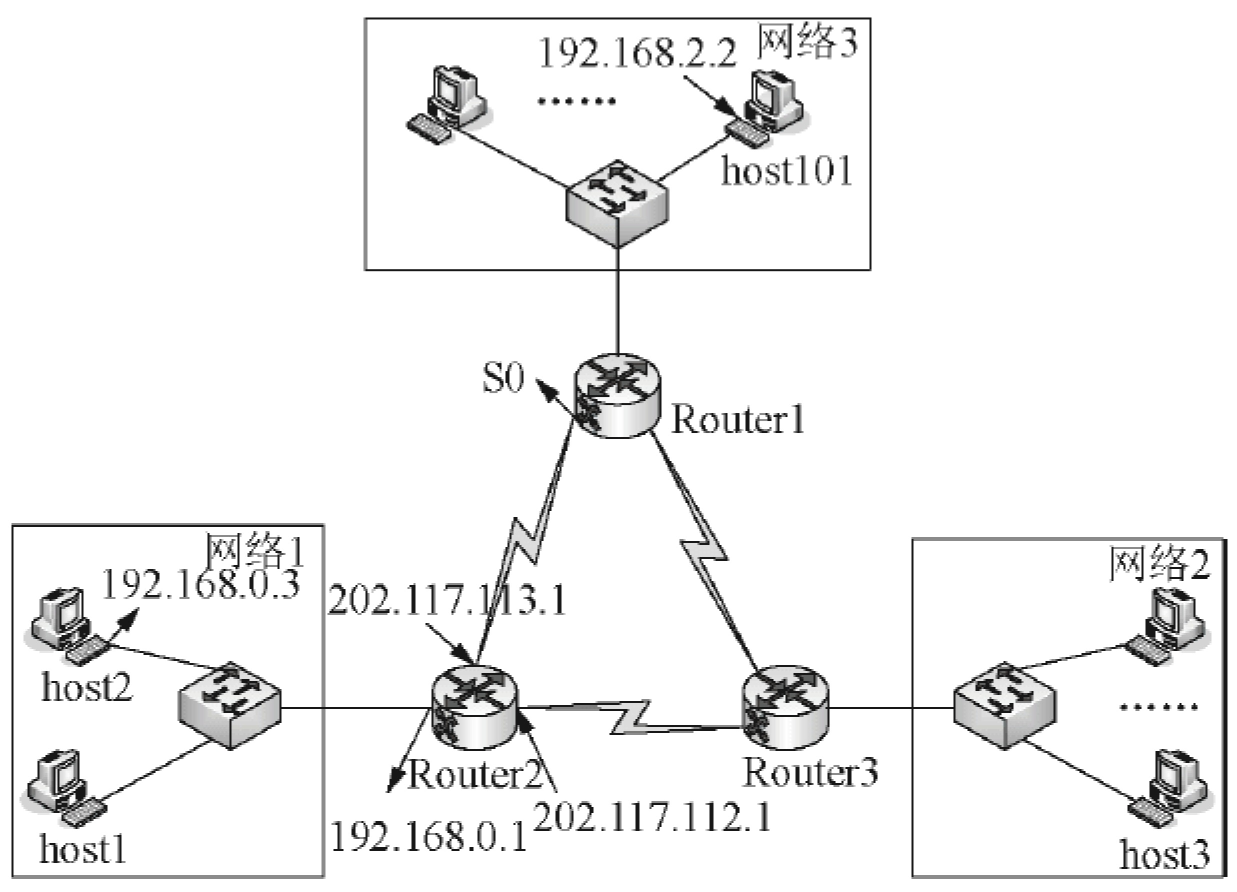


图 5.18 网络拓扑结构

(26) A. 仅网络 1

B. 网络 1、202.117.112.0/30 和 202.117.113.0/30

C. 网络 1、网络 2 和网络 3

D. 仅 202.117.112.0/30 和 202.117.113.0/30

参考答案：(26)B。

要点解析：RIP 协议基于距离矢量路由算法，距离矢量路由算法每次更新路由时发送它的整个路由表，但仅仅给它的邻居，也就是直连与其相邻的网络和路由器。Router2 与路由器 Router1、路由器 Router3 和网络 1 直接相邻。

试题 84 (2015 年上半年试题 28)

有较高实时性要求的应用是__(28)__。

(28) A. 电子邮件　　B. 网页浏览　　C. VoIP　　D. 网络管理



参考答案：(28)C。

要点解析：VoIP 即网络电话，将模拟的声音信号经过压缩与封包之后，以数据封包的形式在 IP 网络进行语音信号的传输，通俗来说也就是互联网电话或 IP 电话。显然，VoIP 网络电话对实时性的要求较高。

试题 85　(2015 年上半年试题 51)

由 DHCP 服务器分配的默认网关地址是 192.168.5.33/28，__(51)__是本地主机的有效地址。

(51) A. 192.168.5.32　　B. 192.168.5.55
C. 192.168.5.47　　D. 192.168.5.40

参考答案：(51)D。

要点解析：网关地址为 192.168.5.33/28，则主机可用 IP 地址为 192.168.5.33～192.168.5.46。192.168.5.32 为子网地址，192.168.5.47 为广播地址。

试题 86　(2015 年上半年试题 52)

如果指定的地址掩码是 255.255.254.0，则有效的主机地址是__(52)__。

(52) A. 126.17.3.0　　B. 174.15.3.255
C. 20.15.36.0　　D. 115.12.4.0

参考答案：(52)A。

要点解析：由地址掩码 255.255.254.0 可知，IP 地址的前 23 位对应网络号，后 9 位对应主机号。选项 B 的主机号部分全为 1，表示广播地址；选项 C 和 D 中的地址后 9 位都为 0，为网络地址。

试题 87　(2015 年上半年试题 59)

如果在网络的入口处通过设置 ACL 封锁了 TCP 和 UDP 端口 21、23 和 25，则能够访问该网络的应用是__(59)__。

(59) A. FTP　　B. DNS　　C. SMTP　　D. Telent

参考答案：(59)B。

要点解析：FTP 使用的是 TCP 的 21 端口，DNS 使用的是 UDP 的 53 端口，SMTP 使用的是 TCP 的 25 端口，Telnet 使用的是 TCP 的 23 端口。

试题 88　(2015 年上半年试题 61)

参见图 5.19 所示的网络连接图，4 个选项是 Host A 的 ARP 表，如果 Host A ping Host B，则 ARP 表中的哪一选项用来封装传输的帧？__(61)__

	Interface Address	Physical Address	Type
A.	192.168.4.7	000f 2480 8916	dynamic
B.	192.168.4.7	0010 5a0c feae	dynamic
C.	192.168.6.2	0010 5a0c feae	dynamic
D.	192.168.6.1	000f 2480 8916	dynamic

参考答案：(61)D。

要点解析：主机如果需要发送数据到与自身不同网段的地址时，它会将数据包发给网关，靠网关来帮它转发。一开始的时候主机是通过 ARP 协议来寻找网关的 MAC 地址的，获得网关的 MAC 地址后，主机就可以直接把数据包发给网关了。

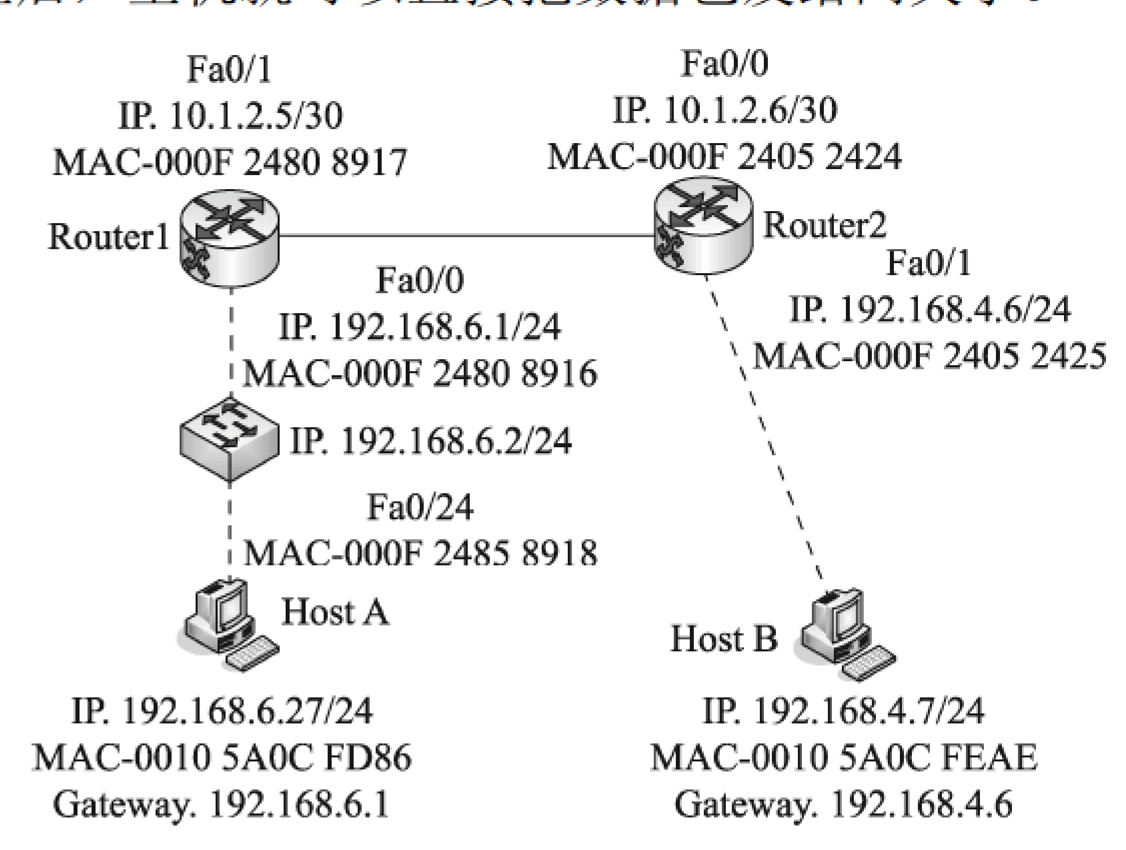


图 5.19　网络连接图

试题 89　(2015 年上半年试题 65)

一个中等规模的公司，3 个不同品牌的路由器都配置了 RIPv1 协议。ISP 为公司分配的地址块为 201.113.210.0/24。公司希望通过 VLSM 技术把网络划分为 3 个子网，每个子网中有 40 台主机，下面的配置方案中最优的是__(65)__。

(65) A. 转换路由协议为 EIGRP，3 个子网地址分别设置为 201.113.210.32/27、201.113.210.64/27 和 201.113.210.92/27

B. 转换路由协议为 RIPv2，3 个子网地址分别设置为 201.113.210.64/26、 201.113 210.128/26 和 201.113.210.192/26

C. 转换路由协议为 OSPF，3 个子网地址分别设置为 201.113.210.16/28、201.113.210.32/28 和 201.113.210.48/28

D. 保持路由协议为 RIPv1，3 个子网地址分别设置为 201.113.210.32/26、201.113. 210.64/26 和 201.113.210.92/26

参考答案：(65)B。

要点解析：RIPv1 不支持可变长子网掩码，RIPv2 支持，因此需要使用 RIPv2 路由协议。由题目知，公司网络被划分为 3 个子网，因此子网位号 2 位(2^2=4)，因此网络号和子网号共占 26 位，得出其掩码为/26。

5.4　强化训练

5.4.1　综合知识试题

试题 1　(2014 年下半年试题 22 和试题 23)

边界网关协议 BGP4 被称为路径矢量协议，它传送的路由信息是由一个地址前缀后



跟__(22)__组成，这种协议的优点是__(23)__。

(22) A. 一串 IP 地址　　B. 一串自治系统编号
　　C. 一串路由器编号　　D. 一串子网地址

(23) A. 防止域间路由循环　　B. 可以及时更新路由
　　C. 便于发现最短通路　　D. 考虑了多种路由度量因素

试题 2　(2014 年下半年试题 24)

与 RIPv2 相比，IGRP 协议增加了一些新的特性，下面的描述中错误的是__(24)__。

(24) A. 路由度量不再把跳步数作为唯一因素，还包含了带宽、延迟等参数
　　B. 增加触发更新来加快路由收敛，不必等待更新周期结束再发送更新报交
　　C. 不但支持相等费用负载均衡，而且支持不等费用的负载均衡
　　D. 最大跳步数由 15 跳扩大到 255 跳，可以支持更大的网络

试题 3　(2014 年下半年试题 25)

为了解决 RIP 协议形成路由环路的问题可以采用多种方法，下面列出的方法中效果最好的是__(25)__。

(25) A. 不要把从一个邻居学习到的路由发送给那个邻居
　　B. 经常检查邻居路由器的状态，以便及时发现断开的链路
　　C. 把从邻居学习到的路由设置为无限大，然后再发送给那个邻居
　　D. 缩短路由更新周期，以便出现链路失效时尽快达到路由无限大

试题 4　(2014 年下半年试题 53)

以下地址中属于自动专用 IP 地址(APIPA)的是__(53)__。

(53) A. 224.0.0.1　　B. 127.0.0.1　　C. 192.168.0.1　　D. 169.254.1.15

试题 5　(2014 年下半年试题 54)

公司得到一个 B 类网络地址块，需要划分成若干个包含 1000 台主机的子网，则可以划分成__(54)__个子网。

(54) A. 100　　B. 64　　C. 128　　D. 500

试题 6　(2014 年下半年试题 55)

IP 地址 202.117.17.254/22 是什么地址？__(55)__

(55) A. 网络地址　　B. 全局广播地址　　C. 主机地址　　D. 定向广播地址

试题 7　(2014 年下半年试题 56)

把下列 8 个地址块 20.15.0.0～20.15.7.0 聚合成一个超级地址块，则得到的网络地址是__(56)__。

(56) A. 20.15.0.0/20　　B. 20.15.0.0/21　　C. 20.15.0.0/16　　D. 20.15.0.0/24

试题 8　(2014 年下半年试题 61)

如果一个 TCP 连接处于 ESTABLISHED 状态，这是表示__(61)__。

(61) A. 已经发出了连接请求　　B. 连接已经建立
　　C. 处于连接监听状态　　D. 等待对方的释放连接响应

试题 9 (2014 年上半年试题 16 和试题 17)

IPv4 的 D 类地址是组播地址，用作组标识符，其中 224.0.0.1 代表__(16)__，224.0.0.5 代表__(17)__。

(16)、(17) A. DHCP 服务器　　B. RIPv2 路由器
C. 本地子网中的所有主机　　D. OSPF 路由器

试题 10 (2014 年上半年试题 18)

按照 IETF 定义的区分服务(DiffServ)技术规范，边界路由器要根据 IP 协议头中的__(18)__字段为每个 IP 分组打上一个称为 DS 码点的标记，这个标记代表了该分组的 QoS 需求。

(18) A. 目标地址　　B. 源地址　　C. 服务类型　　D. 段偏置值

试题 11 (2014 年上半年试题 19 和试题 20)

ICMP 协议属于因特网中的__(19)__协议，ICMP 协议数据单元封装在__(20)__中传送。

(19) A. 数据链路层　　B. 网络层　　C. 传输层　　D. 会话层
(20) A. 以太帧　　B. TCP 段　　C. UDP 数据报　　D. IP 数据报

试题 12 (2014 年上半年试题 21 和试题 22)

TCP/IP 网络中最早使用的动态路由协议是__(21)__协议，这种协议基于__(22)__算法计算路由。

(21) A. RIP　　B. OSPF　　C. PPP　　D. IS-IS
(22) A. 路由信息　　B. 链路状态　　C. 距离矢量　　D. 最短通路

试题 13 (2014 年上半年试题 30)

与 HTTP 1.0 相比，HTTP 1.1 的优点不包括__(30)__。

(30) A. 减少了 RTTs 数量　　B. 支持持久连接
C. 减少了 TCP 慢启动次数　　D. 提高了安全性

试题 14 (2014 年上半年试题 51)

校园网连接运营商的 IP 地址为 202.117.113.3/30，本地网关的地址为 192.168.1.254/24，如果本地计算机采用动态地址分配，在图 5.20 中应如何配置？__(51)__

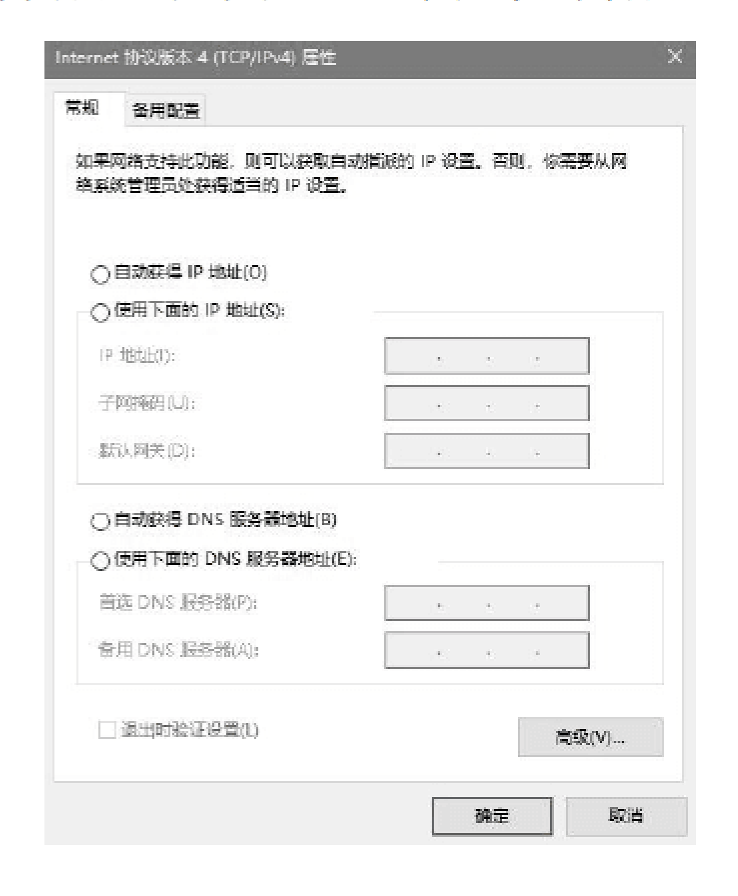


图 5.20　地址分配界面

(51) A. 选取“自动获取 IP 地址”
B. 配置本地计算机 IP 地址为 192.168.1.X
C. 配置本地计算机 IP 地址为 202.115.113.X
D. 在网络 168.254. X. X 中选取一个不冲突的 IP 地址

试题 15 (2014 年上半年试题 52)

下列选项中，不属于网络 202.113.100.0/21 的地址是 (52) 。

(52) A. 202.113.102.0　　B. 202.113.99.0
C. 202.113.97.0　　D. 202.113.95.0

试题 16 (2014 年上半年试题 53 和试题 54)

IP 地址块 112.56.80.192/26 包含了 (53) 个主机地址，不属于这个网络的地址是 (54) 。

(53) A. 15　　B. 32　　C. 62　　D. 64
(54) A.112.56.80.202　　B.112.56.80.191
C.112.56.80.253　　D.112.56.80.195

试题 17 (2014 年上半年试题 55)

下面的地址中属于单播地址的是 (55) 。

(55) A. 125.221.191.255/18　　B. 192.168.24.123/30
C. 200.114.207.94/27　　D. 224.0.0.23/16

试题 18 (2014 年上半年试题 64 和试题 65)

OSPF 协议将其管理的网络划分为不同类型的若干区域(Area)，其中标准区域的特点是 (64) ；存根区域(stub)的特点是 (65) 。

(64) A. 不接收本地 AS 之外的路由信息，也不接收其他区域的路由汇总信息
B. 不接收本地 AS 之外的路由信息，对本地 AS 之外的目标采用默认路由
C. 可以接收任何链接路由更新信息和路由汇总信息
D. 可以学习其他 AS 的路由信息，对本地 AS 中的其他区域采用默认路由
(65) A. 不接收本地 AS 之外的路由信息，也不接收其他区域的路由汇总信息
B. 不接收本地 AS 之外的路由信息，对本地 AS 之外的目标采用默认路由
C. 可以接收任何链接路由更新信息和路由汇总信息
D. 可以学习其他 AS 的路由信息，对本地 AS 中的其他区域采用默认路由

试题 19 (2014 年上半年试题 66 和试题 67)

NAT 技术解决了 IPv4 地址短缺的问题，假设内网的地址数是 m，而外网的地址数是 n，若 $m>n$，则这种技术叫作 (66) ，若 $m>n$，且 $n=1$，则这种技术叫作 (67) 。

(66)、(67) A. 动态地址翻译　　B. 静态地址翻译
C. 地址伪装　　D. 地址变换

试题 20 (2014 年上半年试题 68 和试题 69)

CIDR 技术解决了路由缩放问题。例如 2048 个 C 类网络组成一个地址块，网络号为

192.24.0.0～192.31.255.0，这样的超网号应为 (68) ，其地址掩码应为 (69) 。

(68) A. 192.24.0.0　　B. 192.31.255.0
C. 192.31.0.0　　D. 192.24.255.0

(69) A. 255.255.248.0　　B. 255.255.255.0
C. 255.255.0.0　　D. 255.248.0.0

5.4.2 综合知识试题参考答案

【试题 1】答　案：(22) B；(23) A。

解　析：边界网关协议(BGP)是运行于 TCP 上的一种自治系统间路由协议。BGP 是唯一设计来处理因特网大小的协议，也是唯一能够妥善处理好非路由主机多路连接的协议。BGP4 提供了一套新的机制支持无类域间路由。这些机制包括支持网络前缀的广播、取消 BGP 网络中“类”的概念。BGP4 也引入机制支持路由聚合，包括 AS 路径的聚合。这些改变为建议的超网方案提供了支持。

【试题 2】答　案：(24) B。

解　析：RIPv2 与 IGRP 的区别：

(1) 使用算法不同，IGRP 使用 DUAL 算法，RIPv2 使用 Bellman-Ford 的 DV 算法。

(2) 度量值不同，IGRP 采用复合度量值(带宽、时延、可靠性、负载、MTU)，RIPv2 仅采用跳数作度量，而且有最大跳数(16 跳)的限制。

(3) 组播地址不同，IGRP 为 224.0.0.10，RIPv2 为 224.0.0.9。

(4) 管理距离不同，IGRP 为 90(当然 IGRP summary 为 5)，RIPv2 为 120，也即 IGRP 计算的路由条目可信度要比 RIPv2 高。

(4) 工作层次不同，IGRP 可以看作工作在网络层，而 RIPv2 则是使用 UDP 520 的应用层(由于 RIP 使用 UDP 的关系也导致了其数据包的发送可靠性的保证相对较低，而 IGRP 则有重传等可靠性机制)。

(6) IGRP 支持非等价负载均衡(通过修改 variance 值)，RIPv2 仅为等价负载均衡。

(7) IGRP 能够定义不同的 IGRP AS，RIPv2 不能且也不支持多进程。

(8) 根据算法及运行原理的不同，IGRP 与 RIPv2 的 timer 也会有所不同，IGRP 主要为 hello(5s/60s)，holddown(15s/180s)；RIPv2 为 Update(25.5～30s)，invalid(180s)，flush(240s)，holddown(180s)。而且 IGRP 可根据拓扑表的后备路由对路由的失效进行搜索快速的收敛，RIPv2 则没有这类表以及这些能力。

总体来说，RIPv2 相对于 IGRP 来说，应该应用在网络规模较小、扩展性要求不太高的网络。

【试题 3】答　案：(25)A。

解　析：距离矢量法算法要求相邻的路由器之间周期性地交换路由表，并通过逐步交换把路由信息扩散到网络中所有的路由器。这种逐步交换过程如果不加以限制，将会形成路由环路(Routing Loops)，使得各个路由器无法就网络的可到达性取得一致。

解决路由环路问题可以采用水平分割法(Split Horizon)。这种方法规定，路由器必须有选择地将路由表中的信息发送给邻居，而不是发送整个路由表。具体地说，一条路由信息



不会被发送给该信息的来源。如果每一条路由信息都不会通过其来源接口向回发送，这样就可以避免环路的产生。

简单的水平分割方案是："不能把从邻居学习到的路由发送给那个邻居"，带有反向毒化的水平分割方案(Split Horizon with Poisoned Reverse)是："把从邻居学习到的路由费用设置为无限大，并立即发送给那个邻居。"采用反向毒化的方案更安全一些，可以立即中断环路。相反，简单水平分割方案则必须等待一个更新周期才能中断环路的形成过程。

另外，触发更新技术也能加快路由收敛，如果触发更新足够及时，则也可以防止环路的形成。

【试题 4】答　案：(53)D。

解　析：如果设置了使用 DHCP 获取 IP 地址，当网络中没有架设 DHCP 服务器，或者 DHCP 服务器出了问题的时候，操作系统会自动赋予本机一个类似 169.254.x.x 的 IP 地址。IANA 是负责全球 Internet 的 IP 地址编号分配的机构，它把 169.254.0.0～169.254.255.255 定义为自动专用 IP 地址，这些地址将不能在 Internet 上使用，所以保证不会与其他 Internet 上的 IP 地址冲突。

【试题 5】答　案：(54)B。

解　析：$(2^{16}-2)/1000=64$。

Internet 的 IP 地址空间容量如表 5.6 所示。

表 5.6　Internet 的 IP 地址空间容量

IP 地址类型	第一字节十进制范围	二进制固定最高位	二进制网络位数	网络数	二进制主机位数	主机数
A 类	0～127	0	8	126	24	$2^{24}-2$
B 类	128～191	10	16	2^{14}	16	$2^{16}-2$
C 类	192～223	110	24	2^{21}	8	$2^{8}-2$
D 类	224～239	1110	组播地址			
E 类	240～255	11110	保留给实验使用			

【试题 6】答　案：(55)C。

解　析：判断一个 IP 地址是否为单播地址，只需要看其主机位是否不为全 0 和不为全 1 的情况，主机位全 0 表示网络 ID，主机位全 1 表示局部广播地址。本题中主机地址位为：32−22=10，换成二进制为 0111111110，所以为主机地址。

【试题 7】答　案：(56)B。

解　析：汇聚方法为：

(1)　将各子网地址的网段以二进制写出。

(2)　从第 1 位比特开始进行比较，将从开始不相同的比特到末尾位填充为 0。由此得到的地址为汇总后的网段的网络地址，其网络位为连续相同的比特位数。

7.0 的二进制表示为：00000111 00000000

0.0 的二进制表示为：00000000 00000000

8 个地址块前 21 位相同，从第 22 位开始不同，因此汇聚后的网络地址为 20.15.0.0/21。

【试题 8】答　案：(61)B。

解　析：TCP 状态说明：

(1) LISTENING 状态：FTP 服务启动后首先处于侦听(LISTENING)状态。

(2) ESTABLISHED 状态：ESTABLISHED 的意思是建立连接。表示两台机器正在通信。

(3) CLOSE_WAIT：对方主动关闭连接或者网络异常导致连接中断，这时我方的状态会变成 CLOSE_WAIT，此时我方要调用 close()来使得连接正确关闭。

(4) TIME_WAIT：我方主动调用 close()断开连接，收到对方确认后状态变为 TIME_WAIT。

(5) SYN_SENT 状态：表示请求连接，当你要访问其他计算机的服务时首先要发个同步信号给该端口，此时状态为 SYN_SENT，如果连接成功了就变为 ESTABLISHED，此时 SYN_SENT 状态非常短暂。

【试题 9】答　案：(16)C；(17)D。

解　析：IPv4 的 D 类地址是组播地址，用作一个组的标识符，其地址范围是 224.0.0.0～239.255.255.255。按照约定，D 类地址被划分为 3 类：

224.0.0.0～224.0.0.255：保留地址，用于路由协议或其他下层拓扑发现协议，以及维护管理协议等，例如 224.0.0.1 代表本地子网中的所有主机，224.0.0.2 代表本地子网中的所有路由器，224.0.0.5 代表所有 OSPF 路由器，224.0.0.9 代表所有 RIP2 路由器，224.0.0.12 代表 DHCP 服务器或中继代理，224.0.0.13 代表所有支持 PIM 的路由器等。

224.0.1.0～238.255.255.255：用于全球范围的组播地址分配，可以把这个范围的 D 类地址动态地分配给一个组播组，当一个组播会话停止时，其地址被回收，以后还可以分配给新出现的组播组。

239.0.0.0～239.255.255.255：在管理权限范围内使用的组播地址，限制了组播的范围，可以在本地子网中作为组播地址使用。

【试题 10】答　案：(18)C。

解　析：区分服务(DiffServ)是 IETF 工作组为了克服 Inter-Serv 的可扩展性差在 1998 年提出的另一个服务模型，目的是制定一个可扩展性相对较强的方法保证 IP 的服务质量。

区分服务体系结构(DiffServ)定义了一种可以在互联网上实施可扩展的服务分类的体系结构。一种“服务”，是由在一个网络内，在同一个传输方向上，通过一条或几条路径传输数据包时的某些重要特征所定义的。这些特征可能包括吞吐率、时延、时延抖动，和／或丢包率的量化值或统计值等，也可能是指其获取网络资源的相对优先权。服务分类要求能适应不同应用程序和用户的需求，并且允许对互联网服务的分类收费。

在 DiffServ 中，定义了一个替换头字段，称为 DS 字段，用来取代现有的 IPv4 TOS(服务类型)和 IPv6 Traffic Class (Octet)。

【试题 11】答　案：(19)B；(20)D。

解　析：ICMP 是 TCP/IP 协议簇的一个子协议，属于网络层协议，主要用于在主机与路由器之间传递控制信息，包括报告错误、交换受限控制和状态信息等。ICMP 报文封装在 IP 数据报中传送，因而不保证可靠地提交。

【试题 12】答　案：(21)A；(22)C。

解　析：Xerox 公司在 20 世纪 70 年代开发的 RIP 协议，是 TCP/IP 网络中所使用的最



早路由协议，现在 RIP 已经成为从 UNIX 系统到各种路由器的必备路由协议。

RIP 协议有以下特点。

(1) RIP 是自治系统内部使用的协议即内部网关协议，使用的是距离矢量算法。

(2) RIP 使用 UDP 的 520 端口进行 RIP 进程之间的通信。

(3) RIP 主要有两个版本：RIPv1 和 RIPv2。RIPv1 协议的具体描述在 RFC1058 中，RIPv2 是对 RIPv1 协议的改进，其协议的具体描述在 RFC 2453 中。

(4) RIP 协议以跳数作为网络度量值。

(5) RIP 协议采用广播或组播进行路由更新，其中 RIPv1 使用广播，而 RIPv2 使用组播。

(6) RIP 协议支持主机被动模式，即 RIP 协议允许主机只接收和更新路由信息而不发送信息。

(7) RIP 支持默认路由传播。

(8) RIP 协议的网络直径不超过 15 跳，适合于中小型网络；为 16 跳时认为网络不可达。

(9) RIPv1 是有路由协议，RIPv2 是无路由协议，即 RIPv2 的报文中含有掩码信息。

【试题 13】答　案：(30) D。

解　析：HTTP1.0，每次请求和响应都需要建立 1 个单独的连接，每次连接只是传输 1 个对象，严重影响客户机和服务器的性能。HTTP1.1 支持持久连接，在一个 TCP 连接上可以传送多个 HTTP 请求和响应，减少了建立和关闭连接的消耗和延迟。

HTTP 1.1 还通过增加更多的请求头和响应头来改进和扩充 HTTP 1.0 的功能。

在 HTTP 1.1 中增加 Host 请求头字段后，实现了在一台 Web 服务器上可以在同一个 IP 地址和端口号上使用不同的主机名来创建多个虚拟 Web 站点。

HTTP 1.1 的持续连接，也需要增加新的请求头来帮助实现。例如，Connection 请求头的值为 Keep-Alive 时，客户端通知服务器返回本次请求结果后保持连接；Connection 请求头的值为 Close 时，客户端通知服务器返回本次请求结果后关闭连接。

HTTP 1.1 还有身份认证机制，许多 Web 站点要求用户提供一个用户名和一口令对才能访问存放在其服务器中的文档，这种要求称为身份认证(authentication)。HTTP 提供特殊的状态码和头部来帮助 Web 站点执行身份认证。

HTTP 1.1 支持文件断点续传，即断点处的字节续传，HTTP 1.0 每次传送文件都是从文件头，即 0 字节处开始。

【试题 14】答　案：(51)A。

解　析：题干中关键文字为“本地计算机采用动态地址分配”，在该环境下，DHCP 客户端的网卡参数配置直接选取“自动获取 IP 地址”即可。至于 DNS 服务器 IP 的设置，也可以选取“自动获得 DNS 服务器地址”或选取“使用下面的 DNS 服务器地址”后，手工配置 DNS 服务器地址。

【试题 15】答　案：(52)D。

解　析：“/21”表示该网络有 21 位网络位，包含前两个八位组和第三个八位组的前五位，第三个八位组的后三位和第四个八位组是主机位，用二进制展开为：

01100 100.00000000，横线部分是主机位，主机位的取值范围是：

01100 100.00000000 →96.0

01100 100.00000001 →96.1

…

01100 111.11111110 ➔103.254

01100 111.11111111 ➔103.255

其中 202.113.96.0/21 为网络 ID，202.113.103.255/21 为局部广播地址，该网络 ID 下真正有效的 IP 地址范围是 202.113.96.1/21～202.113.103.254/21。

【试题 16】答　案：(53)C；(54)B。

解　析：地址块 112.56.80.192/26 包含了 6 位主机地址，所以包含的主机地址为 62 个。

网络地址 112.56.80.192/26 的二进制为：01110000 00111000 01010000 11000000

地址 112.56.80.202 的二进制为：01110000 00111000 01010000 11001010

地址 112.56.80.191 的二进制为：01110000 00111000 01010000 10111111

地址 112.56.80.253 的二进制为：01110000 00111000 01010000 11111101

地址 112.56.80.195 的二进制为：01110000 00111000 01010000 11000011

可以看出，地址 112.56.80.191 不属于网络 112.56.80.192/26

【试题 17】答　案：(55)C。

解　析：判断一个 IP 地址是否为单播地址，只需要看其主机位是否不为全 0 和不为全 1 的情况，主机位全 0 表示网络 ID，主机位全 1 表示局部广播地址。我们以 A 答案为例，“/18”表示网络位为 18 位，那么其主机位为 32−18=14，该 14 位主机包含了第三个 8 位组后 6 位和第四个八位组。A 选项中的 191.255 用二进制展开为：10111111.11111111，由此可见主机位全 1，该地址是一个局部广播地址。B、C、D 选项的鉴别方法类似，最终得出 C 选项的主机位非全 0 和全 1，该地址是一个有效主机 IP 地址。

【试题 18】答　案：(64)C；(65)B。

解　析：OSPF 区域类型划分如下。

(1)　骨干区域(即传输区域)：area 0。

(2)　非骨干区域(即常规区域)：除 area 0 之外的其他所有许可范围内的区域。

非骨干区域又可划分如下。

①　标准区域：即正常传输数据的区域。

②　存根区域(末梢区域)：用外部 AS 的信息进入，即 LSA4、LSA5 类信息进入(5 类信息都用了，要 4 类通告 ASBR 来也没用了)，但 AS 内其他区域的路由信息还能接收。

③　完全存根区域(完全末梢区域)：用外部 AS 进入区域的信息，即 LSA5、LSA4、LSA3 类信息进入。

④　NSSA 区域：用非直连的外部 AS 信息进入，同时会产生 LSA7 类信息在表中表示为 ON2(N2 代表类型 2，默认的是 2，可以改成 1，即 metric-type)。

要注意的是，虽然存根区域和完全存根区域都用了外部 AS 信息和区域间的信息，但是不代表就不可达其他区域或者外部了。其他区域和外部路由在禁用之后都会向相应区域内通告一条默认路由以指向外部，保持可达性。但是 NSSA 区域要我们另外输入命令以保证可达外部 AS。

【试题 19】答　案：(66)A；(67)C。

解　析：NAT(Network Address Translation，网址转换)是将 IP 数据包头中的 IP 地址转换为另一个 IP 地址的过程。在实际应用中，NAT 主要用于实现私有网络访问公共网络的功

能。这种通过使用少量的公有 IP 地址代表较多的私有 IP 地址的方式，将有助于减缓可用 IP 地址空间的枯竭。

NAT 的实现方式有三种，即静态转换 Static NAT、动态转换 Dynamic NAT 和端口多路复用 Over Load。

静态转换是指将内部网的私有 IP 地址转换为公有 IP 地址，IP 地址对是一对一的，是一成不变的，某个私有 IP 地址只转换为某个公有 IP 址。借助于静态转换，可以实现外部网对内部网络中某些特定设备(如服务器)的访问。

动态转换是指将内部网的私有 IP 地址转换为公用 IP 地址时，IP 地址是不确定的，是随机的，所有被授权访问 Internet 上的私有 IP 地址可随机转换为任何可指定的合法 IP 地址。也就是说，只要指定哪些内部地址可以进行转换，以及哪些合法地址作为外部地址时，就可以进行转换。动态转换可以使用多个合法外部地址集。当 ISP 提供的合法 IP 地址略少于网络内部的计算机数量时，可以采用动态转换的方式。

端口多路复用(Port Address Translation，PAT)是指改变外出数据包的源端口并进行端口转换，即端口地址转换。采用端口多路复用方式，内部网络的所有主机均可共享一个合法外部 IP 地址，实现对 Internet 的访问，从而可以最大限度地节约 IP 地址资源。同时，又可隐藏网络内部的所有主机，有效避免来自 Internet 的攻击。因此，目前网络中应用最多的就是端口多路复用方式。

题干中 $m>n$ 时，采用态 NAT，当 $m>n$ 且 $n=1$ 时，采用 NAPT-PT 以及地址伪装。

【试题 20】**答　案**：(68)A；(69)D。

解　析：网络号变化范围是 192.24.0.0～192.31.255.0，我们对这些 C 类网络作路由汇聚。假设该汇聚网络 ID 网络位扩长 n 位后，得到 2048 个标准 C 类网络，再利用公式 2^n 即可求出 n 的值。公式 2^n 可以求出子网个数，题干给出子网个数为 2048，所以代入到公式中 $2^n>2048$，此时 n 的值最小为 11，亦即超网将网络位扩长 11 位后得到 2048 个标准 C 类网络，这些子网的子网掩码长度为 24，该超网原来的子网掩码长度为 24−11=13，十进制表示为 255.248.0.0。192.24.0.0～192.31.255.0 中任何一个网络都是超网下的子网网络 ID，随意抽取一个 IP 与 255.248 作“与”运算即可得到超网网络 ID 为 192.24.0.0/13。

第 6 章 下一代互联网

6.1 备考指南

6.1.1 考纲要求

根据考试大纲中相应的考核要求，在“下一代互联网”知识模块上，要求考生掌握以下方面的内容。

(1) IPv6：IPv6 分组格式、IPv6 地址格式前缀、IPv6 地址分类、IPv6 协议。

(2) 移动 IP：移动 IP 的通信过程，移动 IPv6 的工作机制。

(3) 从 IPv4 向 IPv6 的过渡：隧道技术、双协议栈技术、翻译技术。

6.1.2 考点统计

“下一代互联网”知识模块在历次网络工程师考试试卷中出现的考核知识点及分值分布情况如表 6.1 所示。

表 6.1 历年考点统计表

年 份	题 号	知 识 点	分 值
2017 年下半年	上午：58	IPv6	1 分
	下午：无	无	0 分
2017 年上半年	上午：60、61	IPv6 地址	2 分
	下午：无	无	0 分
2016 年下半年	上午：18	IPv6 链路本地地址	1 分
	下午：无	无	0 分

续表

年　份	题　号	知 识 点	分　值
2016 年上半年	上午：无	无	0 分
	下午：无	无	0 分
2015 年下半年	上午：60、61	IPv6 地址	2 分
	下午：无	无	0 分
2015 年上半年	上午：57、58	IPv6 地址、隧道地址	2 分
	下午：无	无	0 分
2014 年下半年	上午：59、60、66	IPv6 单播地址、任播地址、协议翻译技术	3 分
	下午：无	无	0 分
2014 年上半年	上午：56～59	IPv6 地址格式、IPv6 任播地址、移动 IP	4 分
	下午：无	无	0 分
2013 年下半年	上午：56～59	IPv6 单播地址、IPv4 向 IPv6 过渡的技术	6 分
	下午：无	无	0 分
2013 年上半年	上午：59	IPv6 地址	4 分
	下午：无	无	0 分
2012 年下半年	上午：59	IPv6 地址	6 分
	下午：无	无	0 分
2012 年上半年	上午：59	IPv6 地址	10 分
	下午：无	无	0 分

6.1.3　命题特点

2014 年出版的《网络工程师(第 4 版)》将 IPv6 从“网络互连与互联网”一章中分离出来作为单独的一章，并添加了移动 IP、从 IPv4 向 IPv6 的过渡和下一代互联网的发展等当前主流技术。

IPv6 地址是重点，一般考试中都会出现。

从 IPv4 向 IPv6 的过渡技术也是考核的重点，需要掌握好。

6.2　考点串讲

6.2.1　IPv6

6.2.1.1　IPv4 的局限性

IPv4 的局限性主要表现在：32 位的 IP 地址空间将无法满足因特网迅速增长的要求；不定长的数据报头域处理影响了路由器的性能提高；单调的服务类型处理；缺乏安全性要求的考虑；负载的分段/组装功能影响了路由器处理的效率。

6.2.1.2　IPv6 的主要特点

- 地址长度为 128 位，以支持大规模数量的网络节点。

- IPv6 简化了报头，减少了路由表长度，同时减少了路由器处理报头的时间，降低了报文通过因特网的延迟。
- 增强了选项和扩展功能，使 IPv6 具有更大的灵活性和更强的功能。
- IPv6 对服务质量 QoS 作了定义，IPv6 报文可以标记数据所属的流类型，以便路由器或交换机进行相应的处理。
- IPv6 提供了比 IPv4 更好的安全性保证。

6.2.1.3 IPv6 的表示

IPv6 的地址空间采用 128 位地址长度，几乎可以不受限制地提供地址。

1. IPv6 地址的表示

IPv6 地址的长度为 128 位，使用冒号分开十六进制来表示，例如 21DA:0000:0000:0000:00C2: 0EF0:A57E。

某些 IPv6 地址中可能包含一长串 0。当出现这种情况时，可将连续的 0 压缩，例如上述地址可缩写为 21DA:0:0:0:C2:EF0:A57E；如果有多个连续的 0000，可用双冒号来代替，例如上述地址可进一步缩写成 21DA::C2:EF0:A57E。

2. IPv6 计算机中 IPv4 地址的表示

有两种格式：兼容的和映射的。

兼容地址：96 位 0 和 32 位的 IPv4 地址，用于 IPv6 计算机要将报文发送给另一个 IPv6 计算机，但需要通过 IPv4 的区域。例如，IPv4 地址 2.13.17.14 的兼容的 IPv6 地址是 0::020D:110E。

映射地址：80 位的 0 后面跟着 16 位的 1，再接 32 位的 IPv4 地址，用于 IPv6 计算机给 IPv4 计算机发送报文。例如，IPv4 地址 2.13.17.14 映射的 IPv6 是 0::FFFF:020D:110E。

3. IPv6 地址的分类

IPv6 地址有 3 种基本类型：单播、多播和任意播地址。其中，任意播地址是 IPv6 新增的一种地址类型，任意播的目的站是一组计算机，但数据包在交付时只交付给其中的一个，通常是距离最近的一个。

6.2.1.4 IPv6 数据包的格式

IPv6 数据包有一个 40 字节的基本首部，其后可允许有零个或多个扩展首部，再后面是数据，如图 6.1 所示。

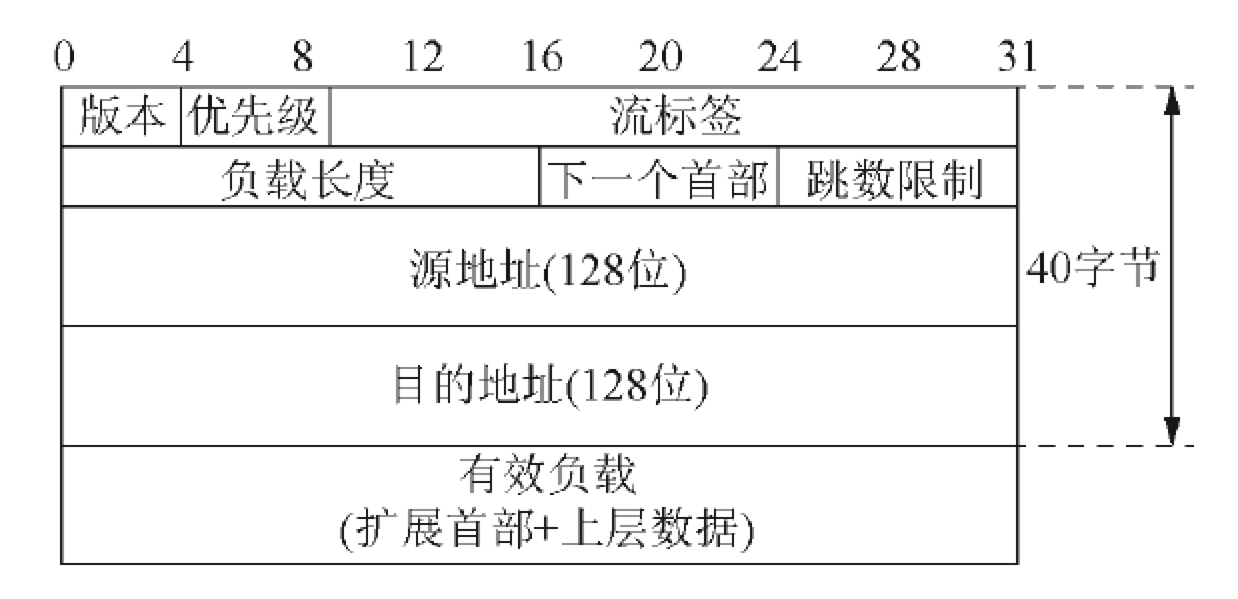
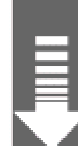


图 6.1 IPv6 数据报



6.2.2　移动 IP

能否在新的联网地点自动重新建立连接，从依赖于固定地点的连接过渡到灵活的移动连接？IETF 给出的解决方案是 RFC 3344 (IP Mobility Support for IPv4)和 RFC 3775 (Mobility Support in IPv6)。

6.2.2.1　移动 IP 的通信过程

RFC 3344 给出的解决方案是增强 IPv4 协议，使其能够把 IP 数据报路由到移动主机当前所在的连接站点。按照这个方案，每个移动主机配置了一个家乡地址(home address)作为永久标识。当移动主机离开家乡网络时，通过所在地点的外地代理，它被赋予了一个转交地址(care-of address)。协议提供了一种注册机制，使得移动主机可以通过家乡地址获得转交地址。家乡代理通过安全隧道可以把分组转发给外地代理，然后被提交给移动主机。

移动 IP 提供了两种获取转交地址的方式。一种是外地代理转交地址(Foreign Agent Care-of Address)，这种转交地址是外地代理在它的代理公告报文中提供的地址，也就是外地代理的 IP 地址。另一种获取模式是配置转交地址(Collocated Care-of Address)，是暂时分配给移动节点的某个端口的 IP 地址，其网络前缀必须与移动节点当前所连接的外地链路的网络前缀相同。一个配置转交地址只能被一个移动节点使用，可以是通过 DHCP 服务器动态分配的地址，或是在地址缓冲池中选取的私网地址。

6.2.2.2　移动 IPv6

RFC 3775 规范了 IPv6 对移动主机的支持功能，定义的协议称为移动 IPv6。移动 IPv6 协议适合于同构型介质，也适合于异构型介质。

1. 移动 IPv6 的工作机制

在移动 IPv6 中，家乡地址是带有移动节点家乡子网前缀的 IP 地址。当移动节点连接在家乡网络中时，发送给家乡地址的分组通过常规的路由机制可以到达移动节点。当移动节点连接到外地链路时，可以通过一个或多个转交地址对其寻址。转交地址是具有外地链路子网前缀的 IP 地址。移动节点可以通过常规的 IPv6 机制获取转交地址。只要移动节点停留在外部某个位置，发送给转交地址的分组都可以被路由到移动节点。当移动节点处于漫游状态时，它可能从几个转交地址接收分组，只要它还能与以前的链路保持连接。

移动节点与对端节点之间的通信有两种方式。第一种方式是双向隧道，这种情况下不需要移动 IPv6 的支持，即使移动节点没有在对端节点上注册，它当前的绑定也可以进行通信。第二种方式是路由优化，要求移动节点把它当前的绑定信息注册到对端节点上，对端节点发出的分组就可以直接路由到移动节点的转交地址。

2. 路由扩展头

RFC 3775 中定义了一种新的 2 型路由头，其中提供的路由地址只具有一个——移动节点的家乡地址。

下一头部	Hdr Ext Len=2	路由类型=2	未用段=1
保留			
家乡地址			

3. 移动扩展头

移动节点、对端节点和家乡代理在生成和管理绑定的过程中都要使用移动头来传输信息。由于为移动头指定的代码是 135，所以在前面的扩展头中要用 135 来指向移动头。

负载的协议	头长度	MH类型	保留
校验和		数据报文	
数据报文			

MH 类型为 8 比特，用于说明报文的类型：
MH=0：绑定刷新请求报文。
MH=1：家乡测试初始化报文。
MH=2：转交测试初始化报文。
MH=3：家乡测试报文。
MH=4：转交测试报文。
MH=5：绑定更新报文。
MH=6：绑定应答报文。
MH=7：绑定出错报文。

6.2.3 从 IPv4 向 IPv6 的过渡

过渡初期要解决的问题可以分成两类：第一类是解决 IPv6 孤岛之间互相通信的问题，第二类是解决 IPv6 孤岛与 IPv4 海洋之间的通信问题。目前提出的过渡技术可以归纳为以下 3 种。

- 隧道技术：用于解决 IPv6 节点之间通过 IPv4 网络进行通信的问题。
- 双协议栈技术：使得 IPv4 和 IPv6 可以共存于同一设备和同一网络中。
- 协议翻译技术：使得纯 IPv6 节点与纯 IPv4 节点之间可以进行通信。

6.2.3.1 隧道技术

所谓隧道，就是把 IPv6 分组封装到 IPv4 分组中，通过 IPv4 网络进行转发的技术。根据隧道端节点的不同，可以分为 4 种不同的隧道：主机到主机的隧道、主机到路由器的隧道、路由器到路由器的隧道、路由器到主机的隧道。

1. 隧道中介技术

隧道中介技术式要求隧道端点必须运行双协议栈，两个端点之间不能使用 NAT 技术，



因为 IPv4 地址必须是全局可路由的。对于 IPv4/IPv6 双栈主机，可以配置一条默认的隧道，以便把不能连接到任何 IPv6 路由器的分组发送出去。双栈边界路由器的 IPv4 地址必须是已知的，这是隧道端点的地址。这种默认隧道建立后，所有的 IPv6 目标地址都可以通过隧道传送。

2. 自动隧道

两个双栈主机可以通过自动隧道在 IPv4 网络中进行通信。实现自动隧道的节点必须采用 IPv4 兼容的 IPv6 地址。当分组进入双栈路由器时，如果目标地址是 IPv4 兼容的地址，分组就被重定向，并自动建立一条隧道。如果目标地址是当地的 IPv6 地址，则不会建立自动隧道。被传送的分组决定了隧道的端点，目标 IPv4 地址取自 IPv6 地址的低 32 位，源地址是发送分组的接口的 IPv4 地址。

3. 6to4 隧道

6to4 是一种支持 IPv6 站点通过 IPv4 网络进行通信的技术，这种技术不需要显式地建立隧道，可以使得一个原生的 IPv6 站点通过中继路由器连接到 IPv6 网络中。

IANA 在可聚合全球单播地址范围内指定了一个格式前缀 0x2002 来表示 6to4 地址。通常把带有 16 位前缀“2002”的 IPv6 地址称为 6to4 地址，而把不使用这个前缀的 IPv6 地址称为原生地址。

中继路由器是一种经过特别配置的路由器，用于在原生 IPv6 地址与 6to4 地址之间进行转换。6to4 技术都是在边界路由器中实现的，不需要对主机的路由配置做任何改变。6to4 路由器应该配置双协议栈，应该具有全局 IPv4 地址，并能实现 6to4 地址转换。这种方法对 IPv4 路由表不增加任何选项，只是在 IPv6 路由表中引入了一个新的选项。

6to4 路由器应该向本地网络公告它的 6to4 前缀 2002:IPv4::/48，其中，IPv4 是路由器的全局 IPv4 地址。在本地 IPv6 网络中的 6to4 主机要使用这个前缀，可以用作自动的地址赋值，或用作 IPv6 路由，或用在 6over4 机制中。

6to4 技术也支持原生 IPv6 站点到 6to4 站点的通信，还可以支持 6to4 站点到原生 IPv6 站点的通信。

4. 6over4 隧道

RFC 2529 定义的 6over4 是一种由 IPv4 地址生成 IPv6 链路本地地址的方法。IPv4 主机的接口标识符是在该接口的 IPv4 地址前面加 32 个“0”形成的 64 位标识符。IPv6 链路本地地址的格式前缀为 FE80::/64，在其后面加上 64 位的 IPv4 接口标识符就形成了完整的 IPv6 链路本地地址。

RFC 2529 规定，IPv6 组播分组要封装在目标地址为 239.192.x.y 的 IPv4 分组中发送，其中 x 和 y 是 IPv6 组播地址的最后两个字节。由于 239.192.0.0/16 是 IPv4 机构本地范围内的组播地址块，所以实现 6over4 主机都要位于同一 IPv4 组播区域内。

IPv6 邻居发现的过程如下：首先 IPv6 主机组播 ICMPv6 邻居邀请报文，然后收到对方的邻居公告报文，其中包含了 64 位的链路层地址。当 IPv6 主机获得了对方主机的 IPv4 地址后，就可以用无状态自动配置方式构造源和目标的链路本地地址，向通信对方发送 IPv6 分组了。当然，IPv6 分组还是要封装在 IPv4 分组中传送的。

5. ISATAP

RFC 4214 定义了一种自动隧道技术——ISATAP，ISATAP 意味着通过 IPv4 地址自动生成 IPv6 站点本地地址或链路本地地址，IPv4 地址作为隧道的端点地址，把 IPv6 分组并封装在 IPv4 分组中进行传送。

一般来说，ISATAP 地址有 64 位的格式前缀，FEC0::/64 表示站点本地地址，FE80::/64 表示链路本地地址。在格式前缀之后要加上修改的 EUI-64 地址，其形式如下：

24 位的 IANA OUI+40 位的扩展标识符

如果 40 位扩展标识符的前 16 位是 0xFFFE，则后面是 24 位的制造商标识符；如果 40 位扩展标识符的前 8 位是 0xFE，则后面是 32 位的 IPv4 地址。

6.2.3.2 协议翻译技术

已经提出的翻译方法有：

- SIIT：无状态的 IP/ICMP 翻译。
- NAT-PT：网络地址翻译-协议翻译。
- SOCKS64：基于 SOCKS 的 IPv6/IPv4 机制。
- TRT：IPv6 到 IPv4 的传输中继翻译器。

1. SIIT

SIIT 转换器规范描述了从 IPv6 到 IPv4 的协议转换机制，包括 IP 头的翻译方法以及 ICMP 报文的翻译方法等。当 IPv6 主机发出的分组到达 SIIT 转换器时，IPv6 分组头被翻译为 IPv4 分组头去，分组的源地址采用 IPv4 翻译地址，目标地址采用 IPv4 映射地址，然后这个分组就可以在 IPv4 网络中传送了。

IPv4 映射地址：一种内嵌 IPv4 地址的 IPv6 地址，可表示为 0:0:0:0:0:FFFF:w.x.y.z 或::FFFF:w.x.y.z 的形式，其中 w.x.y.z 是 IPv4 地址。这种地址用于仅支持 IPv4 的主机。

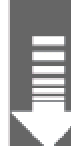
IPv4 翻译地址：一种内嵌 IPv4 地址的 IPv6 地址，可表示为 0:0:0:0:FFFF:0:w.x.y.z 或::FFFF:0:w.x.y.z 的形式，其中 w.x.y.z 是 IPv4 地址。这种地址可用于支持 IPv6 的主机。

2. NAT-PT

NAT-PT 是 RFC 2766 定义的协议翻译方法。实现 NAT-PT 技术必须指定一个服务器作为 NAT-PT 网关，并且要准备一个 IPv4 地址块作为地址翻译之用，要为每个站点至少预留一个 IPv4 地址。

RFC 2766 定义的是有状态的翻译技术，即要记录和保持会话状态，按照会话状态参数对分组进行翻译，包括对 IP 地址及其相关的字段进行翻译。

NAT-PT 操作有 3 个变种：基本 NAT-PT、NAPT-PT 和双向 NAT-PT。基本 NAT-PT 是单向的，只允许 IPv6 主机访问 IPv4 主机；NAPT-PT 也是单向通信，但是扩展到了 TCP/UDP 端口的翻译，也包括 ICMP 询问标识符的翻译，这种技术可以实现从 IPv6 主机的传输标识符到指定 IPv4 地址传输标识符的多路复用，即让一组 IPv6 主机共享同一 IPv4 地址；双向 NAT-PT，这意味着双向通信，无论是 IPv6 主机还是 IPv4 主机，都可协议翻译技术适用于 IPv6 孤岛与 IPv4 海洋之间的通信，这种技术要求一次会话中的双向数据包都在同一个路由器上完成转换，所以它只能适用于同一路由器连接的网络。



6.2.3.3　双协议栈技术

双协议栈技术适用于同时实现了 IPv6 和 IPv4 两个协议栈的主机之间进行通信。在这种情况下，当主机发起通信时，DNS 服务器将同时提供 IPv6 和 IPv4 两种地址，主机将根据具体情况使用适当的协议来建立通信。在服务器一边要同时监听 IPv4 和 IPv6 两种端口。

1. BIS

BIS(Bump-In-the-Stack)是应用于 IP 安全域内的一种机制，适用于在开始过渡阶段利用现有的 IPv4 应用进行 IPv6 通信。这种技术是在主机的 TCP/IPv4 模块与网卡驱动模块之间插入一些模块来实现 IPv4 与 IPv6 分组之间的转换，使得主机成为一个协议转换器。

BIS 用 3 个模块来代替 IPv6 应用：转换器、扩展名解析器和地址映射器。转换器的作用是在 IPv4 地址与 IPv6 地址之间进行转换；扩展名解析器对 IPv4 应用发出的请求返回一个“适当的”答案；地址映射器维护一个 IPv4 地址池，同时维护一个由 IPv4 地址与 IPv6 地址对组成的表。

2. BIA

BIA 是在 IPv4 Socket 应用与 IPv6 Socket 应用之间进行翻译的技术。BIA 要求在 Socket 应用模块与 TCP/IP 模块之间插入 API 转换器，这样建立的双栈主机不需要在 IP 头之间进行翻译，使得转换过程得到简化。API 转换器由 3 个模块组成：功能映射器、名字解析器、地址映射器。功能映射器的作用是在 IPv4 Socket API 功能与 IPv6 Socket API 功能之间进行转换；名字解析器的作用是在收到 IPv4 应用请求时给出适当的响应；地址映射器与 BIS 中的地址映射器相同。

6.2.4　下一代互联网的发展

推动下一代互联网研究的主要因素有 3 个：一是大幅度地增加 IP 地址供给；二是开发新的网络应用；三是抢占 IT 产业竞争优势。

6.2.4.1　IP 地址的分配

IP 地址和 AS 号码的分配主要由美国掌控。ICANN(The Internet Corporation for Assigned Names and Numbers)是负责互联网国际域名、地址和号码管理的非营利性机构。ICANN 将部分 IP 地址和 AS 号码分配给地区级的互联网注册机构 RIR，RIR 再将地址分配给区域内的本地互联网注册机构 LIR 和互联网服务提供商(ISP)，然后由他们向用户分配。

现有 5 个 RIR 管理地区：APNIC 是亚太地区互联网络信息中心；ARIN 是美国网络地址注册管理组织，负责北美地区的 IP 地址和 AS 号码的分配；LACNIC 是拉丁美洲及加勒比地区的互联网络信息中心；RIPE NCC 负责欧洲地区 IP 地址和 AS 号码的管理；AFRINIC 是非洲的网络信息中心。

应对 IPv4 地址的耗尽已成为全球性的战略问题，2006 年，IANA 已经为五大洲的 RIR 分配了全球单播地址格式前缀。

AFRINIC：2C00:0000::/12。

APNIC：2400:0000::/12。

ARIN：2600:0000::/12。

LACNIC：2800:0000::/12。

RIPE NCC：2A00:0000::/12。

6.2.4.2 我国的下一代互联网研究

中国下一代互联网示范工程(CNGI)项目是于2003年启动的。截至目前，CNGI已经建成了由6个主干网、两个国际交换中心及相应的传输链路组成的核心网络。6个主干网是：CERNET2、中国电信、中国网通/中科院、中国移动、中国联通和中国铁通。

1. CERNET2

CERNET2是CNGI中规模最大的主干网，也是目前世界上规模最大的采用纯IPv6技术的下一代互联网。它以2.5G～10Gb/s速率连接全国20个城市的25个主干网核心节点。

2. GLORIAD

2004年1月12日，中美俄环球科教网络(GLORIAD)正式开通，以支持科研、教育方面的国际合作。GLORIAD计划包括下面4个方面的内容。

(1) 网络传输基础设施的研究和建设。设计传输速率为10Gb/s。

(2) 网络重要支撑技术的研究、运行和试验。在网络层将采用IPv6协议实现互连。

(3) 网络应用服务软件和中间件的研究、运行。采用基于网格的软件技术。

(4) 建立强大的科学教育应用联盟。

6.3 真题详解

试题1 (2017年下半年试题58)

以下关于在IPv6中任意播地址的叙述中，错误的是__(58)__。

(58) A. 只能指定给IPv6 路由器　　B. 可以用作目标地址

C. 可以用作源地址　　D. 代表一组接口的标识符

参考答案：(58)C。

要点解析：任意播地址是一个标识符对应多个接口的情况。如果一个数据报文要求被传送到一个任意点地址，则将被传送到最近一个接口(路由器决定)。IPv6任意播地址只能作目标地址而不能作源地址，也不能指定给IPv6主机而只能指定给IPv6路由器。

试题2 (2017年上半年试题60和试题61)

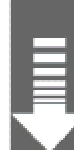
IPv6链路本地单播地址的前缀为__(60)__，可聚集全球单播地址的前缀为__(61)__。

(60) A. 001　B. 1111111010　C. 1111111011　D. 11111111

(61) A. 001　B. 1111111010　C. 1111111011　D. 11111111

参考答案：(60)B；(61)A。

要点解析：链路本地单播地址的格式前缀为1111 1110 10，即FE80::/64，其后是64位的接口ID。IPv6的可聚集全球单播地址是可以在全球范围内进行路由转发的IPv6地址的全



球路由选择前缀；分配给各个公司和机构，用于路由器的路由选择。相当于 IPv4 地址中的网络号，这类地址的前三位是 001。

试题 3　(2016 年下半年试题 18)

IPv6 的链路本地地址是在地址前缀 1111 1110 10 之后附加__(18)__形成的。

(18) A. IPv4 地址　　B. MAC 地址　　C. 主机名　　D. 随机产生的字符串

参考答案：(18)B。

要点解析：IPv6 的链路本地地址是在前缀 1111 1110 10 之后附加 MAC 地址形成的，用于同一链路的相邻节点间通信。链路本地地址相当于 IPv4 中的自动专用 IP 地址(APIPA)，可用于邻居发现，并且总是自动配置的。

试题 4　(2015 年下半年试题 60 和试题 61)

IPv6 地址的格式前缀(FP)用于表示__(60)__。为实现 IP 地址的自动配置，IPv6 主机将__(61)__附加在地址前缀 1111 1110 10 之后，产生一个链路本地地址，如果通过了邻居发现协议的验证，则表明自我配置的链路本地地址是有效的。

(60) A. 地区号　　B. 地址类型或子网地址
C. 网络类型　　D. 播送方式或子网号

(61) A. 32 位二进制随机数　　B. 主机名字
C. 网卡 MAC 地址　　D. IPv4 地址

参考答案：(60)B；(61)C。

要点解析：地址的格式前缀(FP)用于表示地址类型或子网地址，用类似于 IPv4 的 CIDR 表示方法表示。链路本地地址：前缀为 1111 1110 10，用于同一链路的相邻节点间的通信，相当于 IPv4 的自动专用 IP 地址。为实现 IP 地址的自动配置，IPv6 主机将 MAC 地址附加在地址前缀 1111 1110 10 之后，产生一个链路本地地址。

试题 5　(2015 年上半年试题 57)

下面的 4 个 IPv6 地址中，无效地址是__(57)__。

(57) A. ::192:168:0:1　　B. ::2001:3452:4955:2367::
C. 2002:c0a8:101::43　　D. 2003:dead:beef:4dad:23:34:bb:101

参考答案：(57)B。

要点解析：IPv6 地址中一个或多个全 0 字段 0000 可以用一对冒号代替，但不能出现两次代替。

试题 6　(2015 年上半年试题 58)

IPv6 站点通过 IPv4 网络通信需要使用隧道技术，常用的 3 种自动隧道技术是__(58)__。

(58) A. VPN 隧道、PPTP 隧道和 IPSec 隧道
B. 6to4 隧道、6over4 隧道和 ISATAP 隧道
C. VPN 隧道、PPP 隧道和 ISATAP 隧道
D. IPSec 隧道、6over4 隧道和 PPTP 隧道

参考答案：(58)B。

要点解析：自动隧道就是隧道接口中的目的地址可以不用配置，直接从 IPv6 地址中提

取。自动隧道技术主要有6to4隧道技术、6over4隧道技术和ISATAP技术。6to4隧道通过在IPv6报文的目的地址中嵌入IPv4地址，来实现自动获取隧道终点的IPv4地址。6to4隧道采用特殊的6to4地址，其格式为：2002:abcd:efgh:子网号::接口ID/64，其中2002表示固定的IPv6地址前缀，abcd:efgh表示该6to4隧道对应的32位全球唯一的IPv4源地址，用十六进制表示。2002:abcd:efgh之后的部分唯一标识了一个主机在6to4网络内的位置。通过这个嵌入的IPv4地址可以自动确定隧道的终点，使隧道的建立非常方便。6over4隧道机制是将IPv6数据报文前封装上IPv4的报文头，通过隧道(Tunnel)使IPv6报文穿越IPv4网络，实现隔离的IPv6网络的互通。ISATAP使用本地管理的接口标识符::0:5EFE:w.x.y.z，其中::0: 5EFE部分是由Internet号码分配中心(IANA)所分配的机构单元标识符 (00-00-5E)和表示内嵌的IPv4地址类型的类型号(FE)组合而成的。 w.x.y.z部分是任意的单播IPv4地址，既可以是私有地址，也可以是公共地址。

6.4 强化训练

6.4.1 综合知识试题

试题1 (2014年下半年试题59和试题60)

IPv6的可聚合全球单播地址前缀为__(59)__，任意播地址的组成是__(60)__。

(59) A. 010　　B. 011　　C. 001　　D. 100

(60) A. 子网前缀+全0　　B. 子网前缀+全1
C. 链路本地地址前缀+全0　　D. 链路本地地址前缀+全1

试题2 (2014年下半年试题66)

在IPv4和IPv6混合的网络中，协议翻译技术用于__(66)__。

(66) A. 两个IPv6主机通过IPv4网络通信
B. 两个IPv4主机通过IPv6网络通信
C. 纯IPv4主机和纯IPv6主机之间的通信
D. 两个双协议栈主机之间的通信

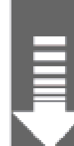
试题3 (2014年上半年试题56)

IPv6地址的格式前缀用于表示地址类型或子网地址，例如60位的地址前缀12AB00000000CD30有多种合法的表示形式，下面的选项中，不合法的是__(56)__。

(56) A. 12AB:0000:0000:CD30:0000:0000:0000:0000/60
B. 12AB::CD30:0:0:0:0/60
C. 12A8:0:0:CD30/60
D. 12AB:0:0:CD30::/60

试题4 (2014年上半年试题57)

IPv6新增加了一种任意播地址，这种地址__(57)__。



(57) A. 可以用作源地址，也可以用作目标地址
B. 只可以作为源地址，不能作为目标地址
C. 代表一组接口的标识符
D. 可以用作路由器或主机的地址

试题 5　(2014 年上半年试题 58 和试题 59)

所谓移动 IP 是指__(58)__；实现移动 IP 的关键技术是__(59)__。

(58) A. 通过地址翻译技术改变主机的 IP 地址
B. 一个主机 IP 地址可以转移给另一个主机
C. 移动主机通过在无线通信网中漫游来保持网络连接
D. 移动主机在离开家乡网络的远程站点可以连接工作

(59) A. 移动主机具有一个可以接入任何网络的通用 IP 地址
B. 移动主机具有一个家乡网络地址并获取一个外地转交地址
C. 移动主机通过控制全网的管理中心申请网络接入服务
D. 移动主机总是通过家乡网络地址获取接入服务

6.4.2　综合知识试题参考答案

【试题 1】答　案：(59)C；(60)A。

解　析：IPv6 地址的格式前缀用于表示地址类型或子网地址，用类似于 IPv4 CIDR 的方法可以表示为“IPv6 地址/前缀长度”的形式。IPv6 地址分为单播地址、组播地址和任意播地址。单播地址又包括可聚合全球单播地址、链路本地地址、站点本地地址和其他特殊单播地址。

可聚合全球单播地址在全球范围内有效，相当于 IPv4 公用地址，其格式前缀为 001。

链路本地地址的有效范围仅限于本地，其格式前缀为 1111 1110 10，用于同一链路的相邻节点间的通信，相当于 IPv4 中的自动专用 IP 地址。

站点本地地址的格式前缀为 1111 1110 11，相当于 IPv4 中的私网地址。

组播地址格式前缀为 1111 1111，此外还有标志、范围和组 ID 等字段。

任意播地址仅用作目标地址，且只能分配给路由器。一个子网内的所有路由器接口都被分配了子网-路由器任意播地址。子网-路由器任意播地址必须在子网前缀中进行预定义。子网前缀必须固定，其余位置全“0”。

【试题 2】答　案：(66)C。

解　析：纯 IPv4 主机和纯 IPv6 主机之间进行通信的需求，由于协议栈的不同，很自然地需要对这些协议进行翻译转换。对于协议的翻译涉及两个方面，一方面是 IPv4 与 IPv6 协议层的翻译，另一方面是 IPv4 应用与 IPv6 协议栈的应用之间的翻译。翻译策略可以对应多种实现技术，其中 NAT-PT 和 TRT 主要应用于网络汇聚层，而 BIA、BIS 则主要是针对主机终端而提出的。

【试题 3】答　案：(56)C。

解　析：此题实际上是考察 IPv6 地址的简写，具体简写方式参考下面的案例。

IPv6 地址为 128 位长，但通常写作 8 组、每组 4 个十六位进制数的形式，例如：

2001:0db8:85a3:0000:1319:8a2e:0370:7344 是一个合法的 IPv6 地址。

如果 4 个数字全都是 0，可以被省略，上例就等价为：

2001:0db8:85a3::1319:8a2e:0370:7344

如果因为省略而出现了两个以上的冒号，则可以压缩为一个，但这种 0 压缩在地址中只能出现一次。

【试题 4】答　案：(57)C。

解　析：任意播(AnyCast)地址是一组接口(可属于不同节点的)的标识符。发往任意播地址的分组被送给该地址标识的接口之一，通常是路由距离最近的接口。对 IPv6 任意播地址存在下列限制：

- 任意播地址不能用作源地址，而只能作为目标地址。
- 任意播地址不能指定给 IPv6 主机，只能指定给 IPv6 路由器。

【试题 5】答　案：(58)D；(59)B。

解　析：Mobile IP 是为了满足移动节点在移动中保持其连接性而设计的。Mobile IP 现在有两个版本，分别为 Mobile IPv4(RFC 3344，取代了 RFC 3220、RFC 2002)和 Mobile IPv6(RFC 3775)。目前广泛使用的仍然是 Mobile IPv4。

简单地说，移动 IP 技术就是让计算机在互联网及局域网中不受任何限制地即时漫游，也称移动计算机技术。

专业来说，移动 IP 技术是移动节点(计算机/服务器/网段等)以固定的网络 IP 地址，实现跨越不同网段的漫游功能，并保证了基于网络 IP 的网络权限在漫游过程中不发生任何改变。

移动 IP 的关键技术有代理搜索、转交地址、登录、隧道。

(1) 代理搜索：是计算节点用来判断自己是否处于漫游状态。

(2) 转交地址：是移动节点移动到外网时从外网代理处得到的临时地址。

(3) 登录：是移动节点到达外网时进行一系列认证、注册、建立隧道的过程。

(4) 隧道：是本地代理与外部代理之间临时建立的双向数据通道。

第 7 章 网络安全

7.1 备考指南

7.1.1 考纲要求

根据考试大纲中相应的考核要求，在“网络安全”知识模块上，要求考生掌握以下方面的内容。

(1) 保密，包括私钥加密体制和公钥加密体制。
(2) 安全体制，包括认证、数字签名、完整性、访问控制。
(3) 安全协议。
(4) 病毒防范和入侵检测。
(5) 访问控制与防火墙，包括 ACL 命令、过滤规则和防火墙配置。
(6) 数字证书。
(7) VPN 配置。
(8) PGP。

7.1.2 考点统计

“网络安全”知识模块在历次网络工程师考试试卷中出现的考核知识点及分值分布情况如表 7.1 所示。

表 7.1 历年考点统计表

年 份	题 号	知 识 点	分 值
2017 年下半年	上午：42、45、65	网络攻击、入侵检测系统	3 分
	下午：试题一	防火墙的配置	20 分

续表

年　份	题　号	知 识 点	分　值
2017 年上半年	上午：37～39、41～45	PGP 协议、IPSec、DES 加密算法、对称密钥密码体制、数字签名、报文摘要算法	8 分
	下午：试题二	防火墙的配置	20 分
2016 年下半年	上午：43～45	数字签名、消息认证算法、对称加密技术	3 分
	下午：试题一	防火墙的配置	20 分
2016 年上半年	上午：41～45	数字证书、对称加密技术、哈希算法和报文鉴别	3 分
	下午：无	无	0 分
2015 年下半年	上午：41～45、47	主动攻击、加密算法、应用层安全协议、防火墙的功能、SSL 安全传输	6 分
	下午：无	无	0 分
2015 年上半年	上午：39～43、64	PGP 协议、入侵检测、宏病毒、Kerberos 算法、三重 DES、拒绝服务攻击	6 分
	下午：无	无	0 分
2014 年下半年	上午：41～45	数字证书、PGP 协议、S-HTTP	5 分
	下午：无	无	0 分
2014 年上半年	上午：41～45	AES 加密算法、报文摘要算法 MD5、IPSec 协议、防火墙、入侵检测	5 分
	下午：无	无	0 分
2013 年下半年	上午：19、20、42～45	CHAP 协议、PKI 体制、报文摘要算法 SHA-1、公开密钥加密算法、DoS 攻击	12 分
	下午：试题二	防火墙的配置	20 分
2013 年上半年	上午：34、41～43	病毒、DES 加密算法、报文摘要算法、PGP 协议	8 分
	下午：无	无	0 分
2012 年下半年	上午：41～44	SSL 协议、SDES 算法、加密和解密	8 分
	下午：无	无	15 分
2012 年上半年	上午：44、45	认证技术、报文摘要算法	4 分
	下午：试题四	IPSec 协议	15 分

7.1.3　命题特点

纵观历年试卷，本章知识点是以选择题和综合分析题的形式出现在试卷中的。本章知识点在历次考试上午试卷中，所考查的题量大约为 7 道选择题，所占分值为 7 分(约占试卷总分值 75 分中的 9%)；在下午试卷中，所考查的题量大约为 1 道综合分析题，所占分值大约为 15 分 (约占试卷总分值 75 分中的 20 %)。本章考题主要检验考生是否理解相关的理论知识点和实践经验，考试难度中等。从知识点考查深度的角度分析，每次考试这部分试题在“识记、理解、应用”3 个层面上所占的比例大致为 1∶1∶2。



7.2 考点串讲

7.2.1 网络安全的基本概念

7.2.1.1 网络安全威胁

网络安全威胁是对网络安全缺陷的潜在利用。这些缺陷可能导致非授权访问、信息泄露、资源耗尽、资源被盗或者被破坏等。网络安全威胁的种类有以下几种。

- 窃听。如搭线窃听、安装通信监视器和读取网上的信息等。
- 假冒。某个实体假装成另一个实体，并获取该实体的权限。
- 重放。重复一份报文或报文的一部分，以便产生一个被授权效果。
- 流量分析。通过对网上信息流的观察和分析推断出网上传输的有用信息。
- 数据完整性破坏。有意或无意地修改或破坏信息系统，或者在非授权和不能检测的方式下对数据进行修改。
- 拒绝服务。通过发送大量的请求来消耗和占用过多的服务资源，使得网络服务不能响应正常的请求。
- 资源的非授权访问。与所定义的安全策略不一致的使用。
- 陷门和特洛伊木马。通过替换系统合法程序，或者在合法程序中插入恶意代码，以实现非授权攻击，从而达到某种特定的目的。
- 病毒。是可执行的恶性程序码，通过对其他程序进行修改，对计算机数据信息进行破坏，抢占系统资源，影响计算机运行速度。
- 诽谤。散布错误的信息以达到诋毁某个对象的形象和知名度的目的。

7.2.1.2 网络攻击

网络攻击是某种安全威胁的具体实现，当信息从信源向信宿流动时，可能受到各种类型的攻击。网络攻击可以分为被动攻击、主动攻击、物理临近攻击、内部人员攻击、分发攻击几类。

1. 被动攻击

被动攻击是对信息的保密性进行攻击，即通过窃听网络上传输的信息并加以分析，从而获得有价值的情报，但它并不修改信息的内容。它的目标是获得正在传送的信息，其特点是偷听或监视信息的传递。主要预防手段是数据加密等。

2. 主动攻击

主动攻击是攻击信息来源的真实性、信息传输的完整性和系统服务的可用性，有意对信息进行修改、插入和删除。主要攻击形式有假冒、重放、欺骗、消息篡改和拒绝服务等。主要预防手段是防火墙、入侵检测技术等。

3. 物理临近攻击

物理临近攻击是未授权者可在物理上接近网络、系统或设备，其目的是修改、收集或

拒绝访问信息。

4. 内部人员攻击

有的内部人员被授权在信息安全处理系统的物理范围内，或对信息安全处理系统具有直接访问权，他们可能会攻击网络。

5. 分发攻击

分发攻击是指在软件和硬件开发出来之后和安装之前这段时间，或者当其从一个地方传到另一个地方时，攻击者恶意修改软硬件。

7.2.1.3 基本安全技术

目前的网络安全措施有：数据加密、数字签名、身份认证、防火墙、入侵检测等。下面章节将对其进行详细的介绍。

7.2.1.4 安全措施的目标

安全措施的目标如下。

- 访问控制。确保会话对方有权做它所声称的事情。
- 认证。确保会话对方的资源同它声称的一致。
- 完整性。确保接收到的信息同发送的信息一致。
- 审计。确保任何发生的交易在事后可以被证实，发信者和收信者都认为交换发生过，即所谓的不可抵赖性。
- 保密。确保敏感信息不被窃听。

7.2.2 数据加密技术

7.2.2.1 加密的基本方法

数据加密的基本思想是通过变换信息的表示形式来伪装需要保护的敏感信息，使非授权者不能了解被加密的内容。需要隐藏的信息称为明文；产生的结果称为密文；加密时使用的变换规则称为密码算法。信息安全的核心是密码技术。

一个加密系统采用的基本工作方式称为密码体制。密码体制的基本要素是密码算法和密钥。其中密码算法可以分为加密算法和解密算法；密钥也相应可以分为加密密钥和解密密钥。

根据密码算法所使用的加密密钥和解密密钥是否相同，可将密码体制分为对称密码体制和非对称密码体制。

- 对称密码体制又称为单密钥体制或隐蔽密钥体制。在这种体制下，加密密钥和解密密钥相同，或者一个可以从另一个导出，拥有加密能力就拥有解密能力；反之亦然。对称密码体制的保密强度高，但开放性差，需要有可靠的密钥传递渠道。
- 非对称密码体制又称为公开密钥体制。在这种体制下，加密和解密的能力是分开的；加密密钥公开，解密密钥不公开，从一个密钥去计算推导另一个密钥是不可行的。非对称密码体制适用于开放的使用环境，密钥管理相对简单，但工作效率一般低于对称密码体制。



加密的基本方法可分为置换和易位两种，实际的算法通常是这两种方法的组合应用。置换改变明文内容的表示形式，但内容元素间的相对位置保持不变；易位改变明文内容元素的相对位置，但保持表示形式不变。

7.2.2.2　数据加密方式

从通信网络的传输方面来看，数据加密技术可以分为 3 类：链路加密方式、节点到节点加密方式和端到端加密方式。

- 链路加密方式是一般网络通信安全主要采用的方式，加密是逐跳进行的，在离开一个节点进入信道时加密，在到达另一端进入下一个节点时解密，因此所有数据在信道中呈现密文形式，在节点中呈现明文形式。
- 节点到节点加密方式是为了解决在节点中数据是明文的缺点，在中间节点里装有加、解密的保护装置，由这个装置来完成一个密钥向另一个密钥的变换。
- 在端到端加密方式中，由发送方加密的数据在没有到达最终目的节点之前是不被解密的，支持这个连接传输的网络信息(如路由信息等)则始终是明文形式，因此对于中继节点而言，用户数据是不可知的密文。

7.2.2.3　对称密钥密码体制

对称密钥加密的发送和接收数据的双方必须使用相同的/对称的密钥对明文进行加密和解密运算。常用的对称加密算法有：DES、IDEA、TDEA、AES、RC2、RC4、RC5 等。

1. 数据加密标准

数据加密标准(Data Encryption Standard，DES)是 20 世纪 70 年代美国联邦注册大会上美国国家标准局(NBS)公开征集的标准密码算法。

DES 属于分组密码体制，它将分组为 64 位的明文加密成 64 位的密文；或反之。整个加密过程由 16 个独立的加密循环所构成，每一个循环使用自己的密钥 $K_1,K_2,\cdots,K_{16}$ 和加密函数。解密使用与加密相同的过程，但顺序与加密相反，从 K_{16} 开始变换，直至 K_1。主密钥为 56 位，用于生成每轮循环各自的密钥 $K_1,K_2,\cdots,K_{16}$。加密函数是 DES 加密运算的核心，分为扩展置换(E 盒)、S 盒置换和后变位(P 盒置换)。

DES 的加密密钥和解密密钥相同，属于对称密码体制，其安全性依赖于密钥。但目前可利用差分密码分析的思想对其选择明文攻击方法，因此 56 位的密钥长度的 DES 原则上不再是安全的。增加密钥长度和采用多重 DES 的加密是有意义的加强办法。

2. 三重 DES

三重 DES 是指使用两个密钥，执行三次 DES 算法，如图 7.1 所示。其密钥长度是 112 位。

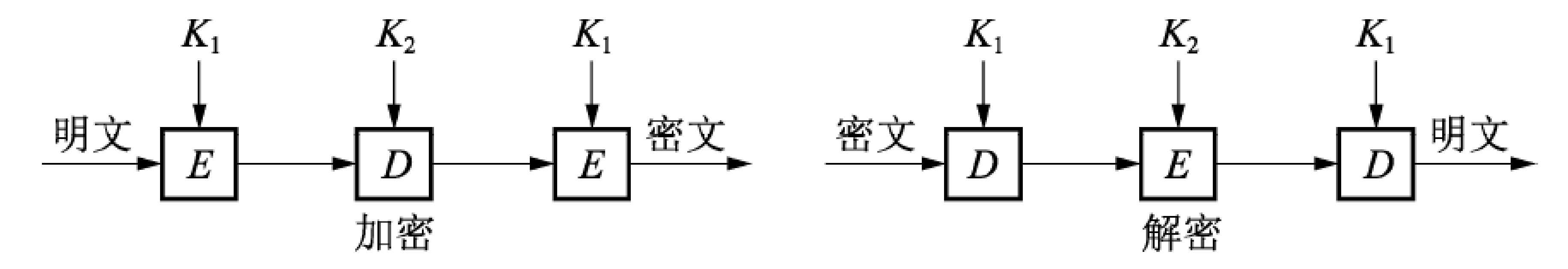


图 7.1　三重 DES 加密算法

3. 国际数据加密数据算法

国际数据加密数据算法(International Data Encryption Algorithm，IDEA)是瑞士苏黎世联邦工业大学(ETH)的Xuejia Lai和James L. Massey于1991年提出的。在算法形式上它和DES类似，也是使用循环加密方式，把分组为64位的明文加密为64位的密文；或反之。所不同的是，IDEA使用128位的密钥，扩展成52个16位循环密钥，安全性强于DES。若采用强行攻击，对付IDEA将是对付DES工作量的$2^{72}=4.7\times10^{21}$倍，因此，它的安全性比较高，是目前数据加密中应用较为广泛的一种密码体制。

由于加密密钥和解密密钥都由同一个主密钥派生而来，IDEA仍属于对称密码体制，而且其设计倾向于软件实现，目前尚未找到破译方法。

7.2.2.4 公开密钥密码体制

公开密钥密码体制也叫非对称密钥加密。每个用户都有一对密钥：公开密钥和私有密钥。公钥对外公开，私钥由个人秘密保存，用其中一把密钥来加密，另一把密钥来解密。虽然解密密钥SK是由公开密钥PK决定的，但不能根据PK计算出SK。其原理如图7.2所示。

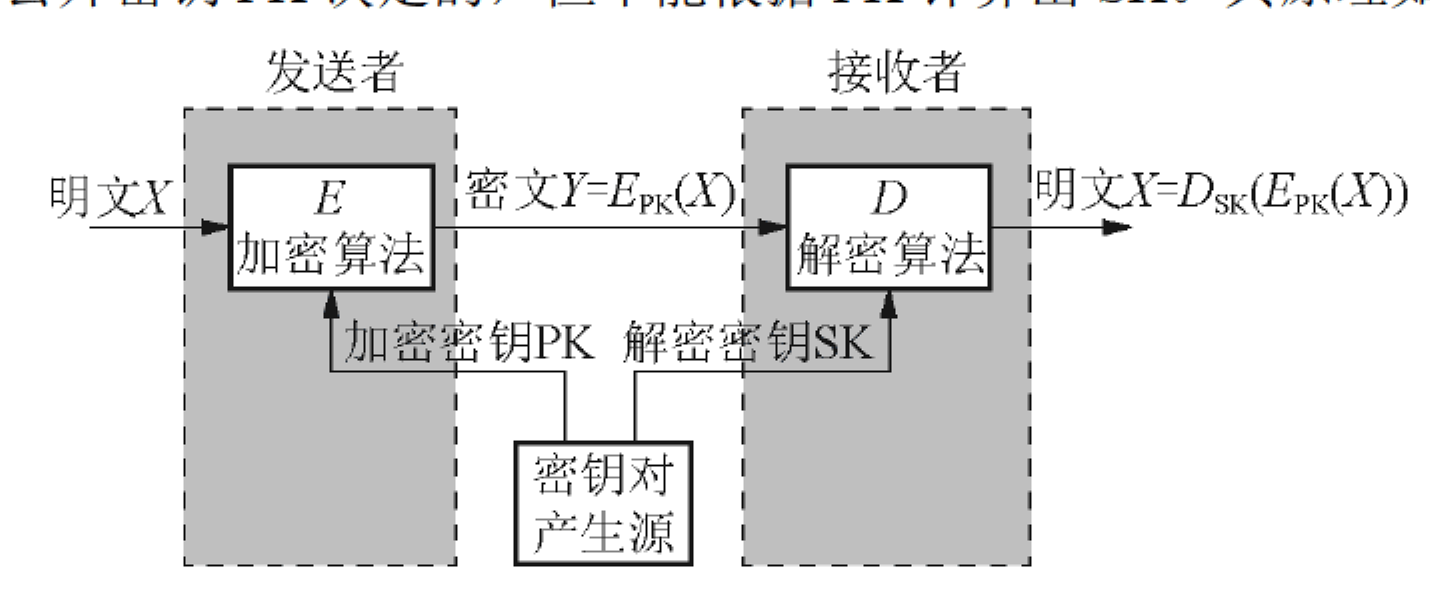


图7.2 公开密钥密码算法

1. RSA算法

RSA是一种非对称分组密码体制，与传统对称密码体制相比，RSA让加密密钥公开称为公钥，而解密密钥隐藏在个体中作为私钥。公钥和私钥在本质上是不同的，由于构造公钥和私钥之间关系的单项函数是NP问题，因此不存在由其中任何一个推导出另一个的算法。在对称密码体制中，由于共享密钥导致使用不同密钥的N个人之间需要$N(N-1)/2$个密钥，密钥量呈非线性增长；而使用RSA，N个人之间则需要N个密钥，密钥量是线性增长的。同时由于私钥带有个人特征，可以解决数据的签名验证问题。

RSA基于大整数的质因子分解问题的困难性，即寻找大整数的质因子是计算不可行的。密钥是变长的，其中明文块的长度应小于等于加密密钥长度，密文长度等于解密密钥长度。由于RSA涉及大数的计算，无论硬件实现还是软件实现效率都比较低，因此它不适用于对长明文进行加密，常用来对密钥进行加密，即与对称密码体制结合使用。

RSA加密之前的准备工作如下。

- 设p、q为质数(由于RSA算法的安全性p和q必须是100位以上的大质数，其判定方法用Fermat定理)。p、q的选择一般是事先由官方提供的大质数，其具体值是保密的。
- 用两个质数的同余运算计算出$r=p*q$。
- 则对应Euler函数为：$\phi(r)=\phi(p)*\phi(q)=(p-1)*(q-1)$。



- 定义 PK 为公钥，SK 为私钥，PK*SK=$m\phi(r)+1$，其中 $m>>1$。
- 设 $X<r$，则有 $X^{SK*PK}=X^{m\phi(r)+1}=(X^m)^{\phi(r)}*X$，所以 X 与 r 互质。
- 根据 Euler 定理：$(X^m)^{\phi(r)}=1\bmod p$。

PK 为公钥，SK 为私钥，X 为明文，Y 为密文，则

加密时：$E_{PK}(X)=Y=X^{PK}\bmod r$。

根据 Euler 定理：$X^{PK*SK}\bmod r=X\bmod r$。

解密时：$D_{SK}(Y)=Y^{SK}\bmod r=(X^{PK})^{SK}\bmod r=X\bmod r$。

由于乘幂的可交换性，RSA 的加密和解密是可以混合进行的。

RSA 是目前国际公开密钥算法的事实标准，得到了广泛承认，一些国家将其作为公开密钥算法的标准。这个算法从 1978 年提出以来，一直是众多密码破译者的目标，但至今还没有发现严重缺陷。

2. 其他的公钥加密算法

ElGamal 算法也是一种常用的公钥加密算法，它是基于公钥密码体制和椭圆曲线加密体系，既能用于数据加密，也能用于数字签名。背包加密算法以其加密、解密速度快而引人注意，但是大多数一次背包体制均被破译了，因此很少有人使用。

7.2.3　认证技术与数字签名

认证可以分为实体认证和消息认证两种。实体认证是识别通信对方的身份，防止假冒，可以使用数字签名的方法。消息认证是验证消息在传送或存储过程中有没有被篡改，通常使用报文摘要的方法。

7.2.3.1　3 种认证技术

1. 基于共享密钥的认证

使用共享密钥的认证方法时，通信双方有一个共享的密钥，要依赖于一个双方都信赖的密钥分发中心(Key Distribution Center，KDC)，其认证过程如图 7.3 所示。A 向 KDC 发出消息(这个消息的一部分用 K_A 加密了)，说明自己要和 B 进行通信，并指出了与 B 会话的密钥 K_S。KDC 知道 A 的意图后构造一个消息发给 B，B 用 K_B 解密后就得到了 A 和 K_S，然后就可以与 A 会话了。

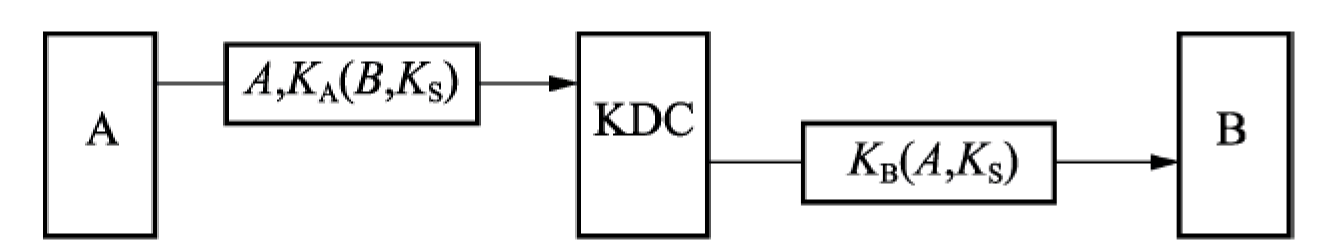


图 7.3　基于共享密钥的认证协议

2. Needham-Schroeder 认证协议

这是一种多次提问-响应协议，可以对付重放攻击，关键是每一个会话回合都有一个新的随机数在起作用，其应答过程如图 7.4 所示。

3. 基于公钥的认证

基于公钥的认证是指通信双方都用对方的公钥加密，用各自的私钥解密，具体过程如

图 7.5 所示。通信报文中有 A 和 B 指定的随机数 R_A 和 R_B，因此能排除重放的可能性。

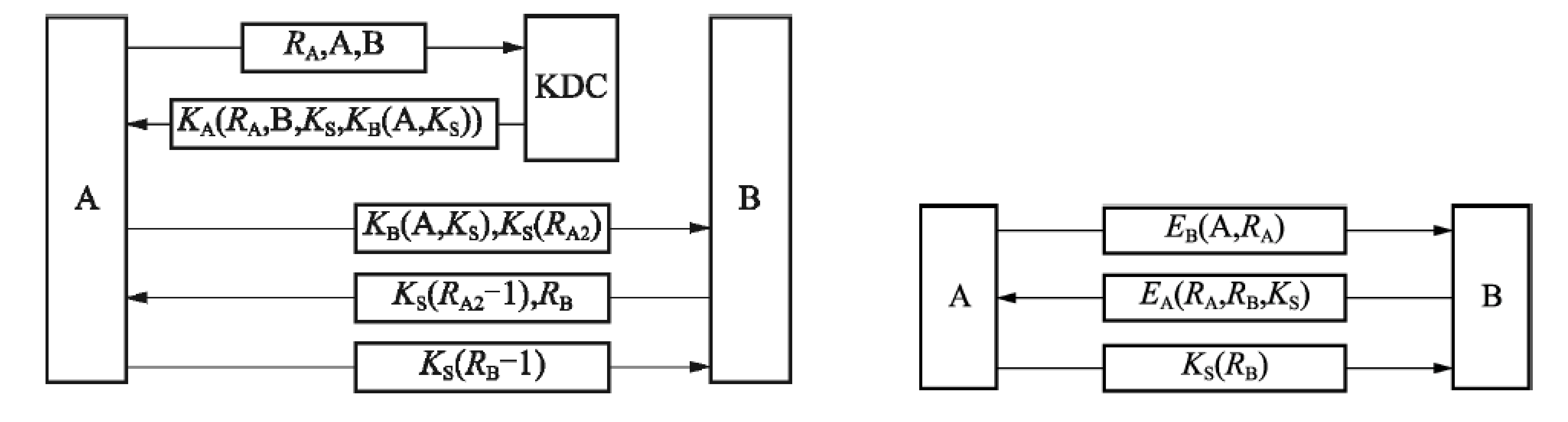


图 7.4　Needham-Schroeder 认证协议　　　图 7.5　基于公钥的认证协议

7.2.3.2　数字签名

数字签名是用于确认发送者身份和消息完整性的一个加密的消息摘要。数字签名应满足以下 3 点：①接收者能够核实发送者；②发送者事后不能抵赖对报文的签名；③接收者不能伪造对报文的签名。

数字签名可以利用对称密码体系(如 DES)、公钥密码体系或公证体系来实现。最常用的实现方法是建立在公钥密码体系和单向散列函数算法(如 MD5、SHA)的组合基础上。

1. 基于密钥的数字签名

基于密钥的数字签名系统中要有收发双方共同信赖的仲裁人，如图 7.6 所示。其中，BB 是 A 和 B 共同信赖的仲裁，K_A 和 K_B 分别是 A 和 B 与 BB 之间的密钥，K_{BB} 是只有 BB 掌握的密钥，P 是 A 发给 B 的消息，t 是时间戳。由 BB 解读 A 发的报文，然后产生一个签名的消息 K_{BB}(A,t,P)，并装配成发给 B 的报文；B 可以解密该报文，阅读消息 P，并保留证据。

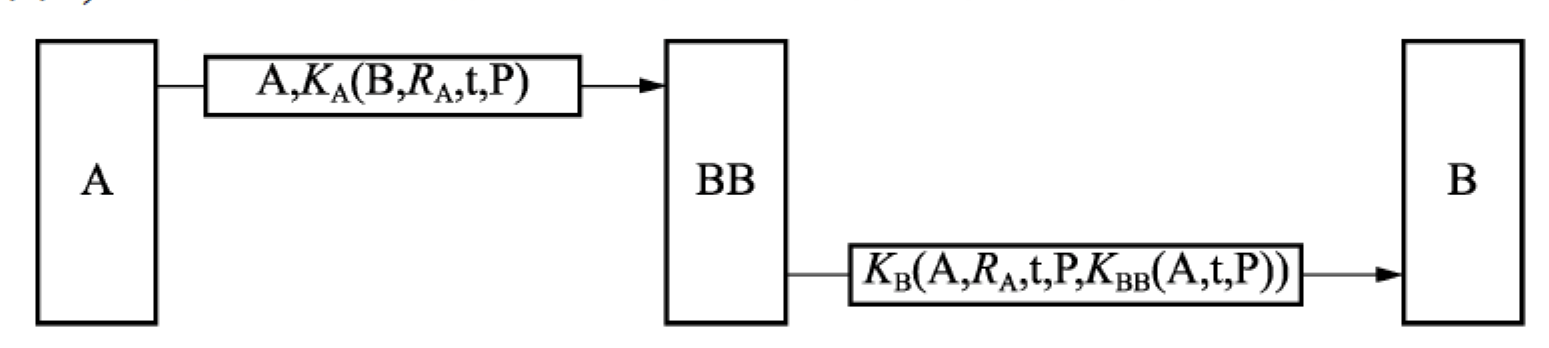


图 7.6　基于密钥的数字签名

2. 基于公钥的数字签名

利用公钥加密算法的数字签名系统如图 7.7 所示。这样的签名方法是符合可靠性原则的，即签字是可以被确认的；签字是无法被伪造的；签字是无法重复使用的；文件被签字以后是无法被篡改的；签字具有无可否认性。如果 A 方否认了，B 可以拿出 D_A(P)，并用 A 的公钥 E_A 解密得到 P，从而证明 P 是 A 发送的；如果 B 把消息篡改了，当 A 要求 B 出示原来的 D_A(P)时，B 拿不出来。

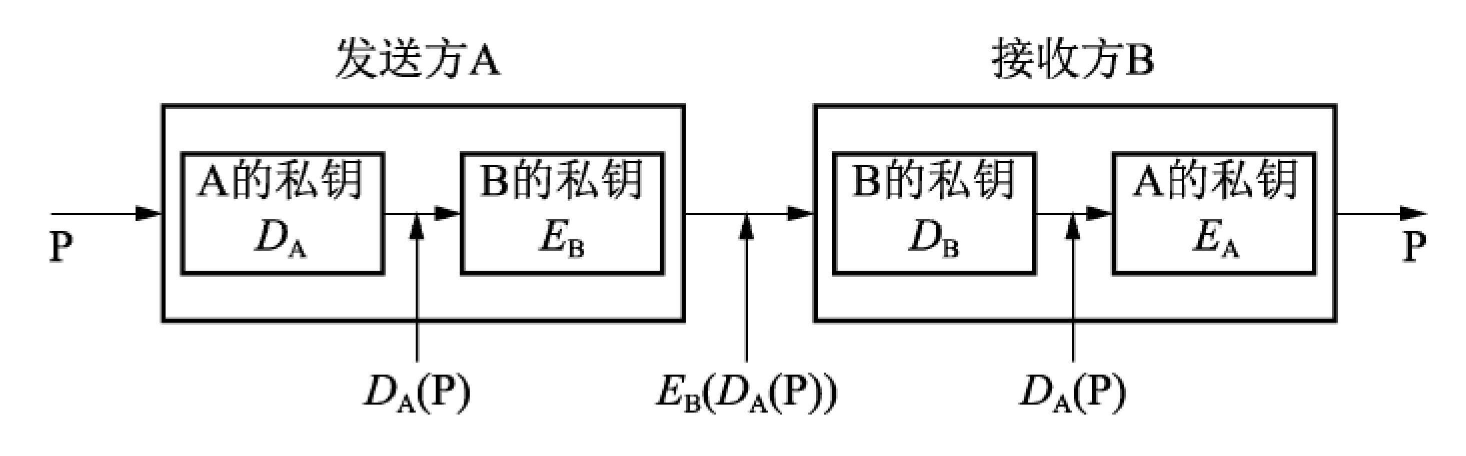


图 7.7　基于公钥的数字签名



7.2.3.3　报文摘要

报文摘要是单向的散列函数，以变长的信息输入，把其压缩成一个定长的值输出。若输入的信息改变了，则输出的定长值(摘要)相应地也会改变。从数据完整性保护的角度来看，报文摘要可为指定的数据产生一个不可仿造的特征，伪造一个报文并使其具有相同的报文摘要是计算不可行的。目前信息摘录的方法主要有 MD5、SHA、HMAC 三种。

1. MD5

MD5 是 MIT 的 Ron Rivest(RFC 1321)提出的。算法以任意长的报文作为输入，算法的输出是产生一个 128 位的报文摘要。输出的摘录用 4 个字 d_0、d_1、d_2、d_3 表示，在计算开始时分别初始化为常数，然后一直参与算法，其值不断被改变，直到作为最后结果输出。

最初值：d_0=01234567H，d_1=89abcdef H，d_2=fedcba98H，d_3=76543210H。

输入报文首先被填充，使其成为 16 的倍数，然后被分成 512 比特的等长块，逐块处理。每块处理分 4 遍扫描，在每遍扫描时对 d_0、d_1、d_2、d_3 使用不同的扰乱函数，扰乱函数将报文的分组和相应 d_i 进行函数运算，这样每遍扫描将每个 d_0、d_1、d_2、d_3 报文内容进行了更新。在处理前将当前摘录备份，在处理后将这个备份加到新产生的信息摘录上，并将其作为下一块处理时的摘录当前值。最后一块信息处理之后的信息摘录 d_0、d_1、d_2、d_3 当前值，即为最终的信息摘录值。

扰乱函数计算使用了取整、二进制求补、二进制与运算、二进制或运算、半加运算、二进制加运算和循环左移运算等。

2. 安全散列算法

安全散列算法(Secure Hash Algorithm，SHA)是由美国标准与技术研究所(NIST)设计并在 1993 年作为联邦信息处理标准的。SHA 的算法建立在 MD5 的基础上，其基本框架与 MD5 类似。其实现思想是将变长信息分成若干个 512 比特的定长块进行处理。与 MD5 有所不同，SHA 输出 160 比特的摘录。

输入摘录为 A、B、C、D、E，各为 32 比特的 5 个字长，分别设初值：A=67452301H；B=efcda89H；C=98badcefH；D=c3d2e1f0H；E=87c3d205H 作为最初的摘录。

算法的核心是具有 4 轮运算的模块，每轮执行 20 步迭代。4 轮运算结构相同，但每轮使用不同的处理函数。每轮的输入是要处理的 512 位报文分组和当前摘录值 A、B、C、D、E，处理时结合报文内容对 A、B、C、D、E 进行更新。每一块与当前信息摘录值结合，产生信息摘录的下一个中间结果，直至处理完毕。

3. 散列式报文认证码

散列式报文认证码(HMAC)是利用对称密钥生产报文认证码的散列算法，可以提供数据完整性、数据源身份认证。

HMAC 使用现有的散列函数 H 而不用修改其代码，这样可以使用已有的 H 代码库，而且可以随时用一个散列函数代替另一个散列函数。HMAC-MD5 已经被 IETF 指定为 Internet 安全协议 IPSec 的验证机制，提供数据源认证和数据完整性保护。

7.2.3.4　数字证书

1. 数字证书的概念

数字证书解决了公开密钥密码体制下密钥的发布和管理问题，用户可以公开其公钥，

而保留其私钥，一般包含用户身份信息、用户公钥信息以及身份验证机构数字签名的数据。

数字证书是一个经证书认证中心(CA)数字签名的包含公开密钥拥有者信息以及公开密钥的文件。认证中心(CA)作为权威的、可信赖的、公正的第三方机构，专门负责为各种认证需求提供数字证书服务。目前得以广泛使用的证书标准是X.509。表7.2所示的是X.509数字证书中的各个数字域的含义。

表7.2　X.509数字证书格式

域	含　义
版本号	证书版本号，不同版本的证书格式不同
序列号	序列号，同一身份验证机构签发的证书序列号唯一
签名算法	签署证书所用的签名算法，包括必要的参数
发行者	建立和签署证书的CA名称
有效期	包括有效期的起始时间和终止时间
主体名	证书持有人的名称，以及这一证书用来证明私钥用户对应的公开密钥
主体的公钥	主体的公开密钥、使用这一公开密钥的算法的标识符及参数
发行者唯一标识符	(可选)证书颁发者的唯一标识符
主体唯一标识符	(可选)证书拥有者的唯一标识符
扩充域	(可选)可选的标准和专用功能字段，如基本限制字段和密钥用法字段
签名	CA用自己的私钥对上述域的哈希值进行数字签名的结果

2. 证书的获取

任何一个用户要得到CA中心的公钥，就能得到该CA中心为该用户签署的公钥。由于证书是不可伪造的，因此对于存放证书的目录无须施加特别保护。

由于一个公钥用户拥有的可信任管理中心数量有限，因此要与大量不同管理域的用户建立安全通信需要CA间建立信任关系。一个证书链是从一个自签名的根证书开始，前一个证书主体是后一个证书的发放者，也就是说，该主体对后一个证书进行签名。一般来说，对证书链的处理需要考虑每个证书相关的信任关系。

3. 证书的吊销

用户的数字到了有效期、用户私钥已被泄露、用户放弃使用原CA中心的服务、CA中心私钥泄露等都需要吊销用户的数字证书。为此，CA维护中心有一个证书吊销列表CRL，以供用户查询。

7.2.3.5　密钥管理

密钥管理是指处理密钥自产生到最终销毁的整个过程中的有关问题，包括系统的初始化，密钥的产生、存储、备份/恢复、装入、分配、保护、更新、控制、丢失、吊销和销毁。

在美国信息保障技术框架(IATF)中定义了密钥管理体制主要有3种：一是适用于封闭网的技术，以传统的密钥分发中心为代表的KMI机制；二是适用于开放网的PKI机制；三是适用于规模化专用网的SPK技术。

PKI本质上是一种公证服务。它通过离线的数字证书来证明某个公开密钥的真实性，并通过证书撤销列表(Certificate Revocation List，CRL)来确认某个公开证书的有效性。



PKI 在宏观上呈现为域结构，即每个 PKI 都有一定的覆盖范围，形成管理域。这些域通过交叉证书相关联，构成更大的管理域。PKI 由政策审批机构(Policy Approval Authority，PAA)、证书管理中心(Certification Authority，CA)、单位注册机构(Organizational Registry Authority，ORA)等部分组成。PAA 制定整个体系结构的安全政策并制定所有下级机构的规章制度；CA 负责具体的证书颁发和管理，它是可信任的第三方；ORA 可以帮助远离 CA 的端实体在 CA 处注册证书。

PKI 框架中有两种端实体：持证者和验证者。持证者向证书管理申请证书用以证明自身身份，从而获得某种权利；验证者通常是授权者，它在确认持证者提供证书的有效性和对方真正身份之后，才会授予对方相应权利。

7.2.4　虚拟专用网

7.2.4.1　虚拟专用网的工作原理

虚拟专用网络(Virtual Private Network，VPN)是一种利用公共网络来构建的专用网络技术，用于构建 VPN 的公共网络，包括 Internet、帧中继、ATM 等。“虚拟”这一概念是相对于传统专用网络的构建方式而言的，对于广域网连接，传统的组网方式通过远程拨号连接来实现，而 VPN 是利用服务提供商所提供的公共网络来实现远程的广域连接。

通常 VPN 整合了范围广泛的客户，从家庭的拨号上网用户到办公室的联网的工作站，直到 ISP 的 Web 服务器。客户类型、传输方法以及使用服务的混合使用增加了 VPN 的设计复杂性，同时也增加了安全需要的复杂性，安全考虑必须同时顾及 VPN 使用的硬件设计和软件。

1. 实现 VPN 的关键技术

实现 VPN 的关键技术主要有：隧道技术、加/解密技术、密钥管理技术和身份认证技术。

- 隧道技术是一种通过使用互联网基础设施在网络之间传递数据的方式。隧道协议将其他协议的数据封装在新的包头中发送。新的包头提供了路由信息，从而使封装的负载数据能够通过互联网传递。
- VPN 可以利用已有的加密技术实现保密通信，保证公司业务和个人通信的安全。
- 密钥管理负责密钥的生成、分发、控制和跟踪以及验证密钥的真实性等。
- 通常使用用户名和密码，或者智能卡实现用户的身份认证。

2. VPN 的解决方案

VPN 的解决方案有以下 3 种。

- Access VPN：用于远程用户需要及时地访问 Intranet 和 Extranet，如出差流动员工、远程办公人员和远程小办公室，通过公用网络与企业的 Intranet 和 Extranet 建立私有的网络连接。通常利用二层网络隧道技术建立 VPN 隧道连接来传输私有网络数据。
- Intranet VPN：通过公用网络进行企业各个分布点的互连，是传统的专线网或其他企业网的扩展或替代形式。
- Extranet VPN：通过一个使用专用连接的共享基础设施，将客户、供应商、合作伙伴或兴趣群体连接到企业内部网。企业拥有与专用网络的相同政策，包括安全、服务质量(QoS)、可管理性和可靠性。

7.2.4.2 第二层隧道协议

虚拟专用网可以通过第二层隧道协议实现，这些隧道协议都是把数据封装在点对点协议(PPP)的帧中在互联网上传输的。下面介绍 PPP 协议和常用的第二层隧道协议。

1. PPP 协议

PPP(Point to Point Protocol，点对点协议)是 IETF 推出的点到点类型线路的数据链路层协议。它解决了 SLIP 中的问题，并成为正式的互联网标准。

PPP 协议定义了 PAP 和 CHAP 两种验证方式，同级系统可以使用这两种认证方式相互进行标识。

2. PPTP 协议

PPTP(点对点隧道协议)是一种第二层隧道协议。为了传输来自不同网络的数据包，最普遍使用的方法是先把各种网络协议(IP、IPX 和 AppleTalk 等)封装到 PPP 中，再把这整个数据包装入隧道协议里。这种双层封装形成的数据包需靠第二层协议进行传输，所以称为“第二层隧道”。

PPTP 定义了由 PAC 和 PNS 组成的客户端/服务器结构，从而把 NAS 的功能分解给这两个逻辑设备，以支持虚拟专用网。

- PAC 即 PPTP 接入集中器(PPTP Access Concentrator)，可以连接一条或多条 PSTN 或 ISDN 拨号线路，能进行 PPP 操作，并能处理 PPTP 协议。
- PNS 即 PPTP 网络服务器(PPTP Network Server)，是建立在通用服务器平台上的 PPTP 服务器，运行 TCP/IP 协议，可以使用任何 LAN 和 WAN 接口硬件实现。

基于 PPTP 协议(点对点隧道协议)网络连接方式的 VPN，允许一台客户机通过一个公共网络(例如 Internet)建立一个秘密的多协议 VLAN 网络，因此，它可以使得公司远端的员工通过 Internet 而不是直接拨号连接公司的网络。这就是说，通过 PPTP 的封装，可以使非 IP 网络获得 Internet 通信的优点。PPTP 是微软公司和其他厂家支持的标准，它是 PPP 协议的扩展，可以通过 Internet 建立多协议 VPN。

3. 第二层隧道协议

第二层隧道协议(Layer 2 Tunneling Protocol，L2TP)是一种基于点对点协议(PPP)的二层隧道协议。L2TP 扩展了 PPP 模型，允许第二层连接端点和 PPP 会话端点驻在由分组交换网连接的不同设备中。L2TP 的典型结构如图 7.8 所示。其中，LAC 表示 L2TP 访问集中器，是附属在交换网络上的具有接入功能和 L2TP 协议处理能力的设备；LNS 是 L2TP 网络服务器，是用于处理 L2TP 协议服务器端部分的软件。在一个 LNS 和 LAC 对之间存在两种类型的连接，一种是隧道(Tunnel)连接，它定义了一个 LNS 和 LAC 对；另一种是会话(Session)连接，它复用在隧道连接之上，用于表示承载在隧道连接中的每个 PPP 会话过程。

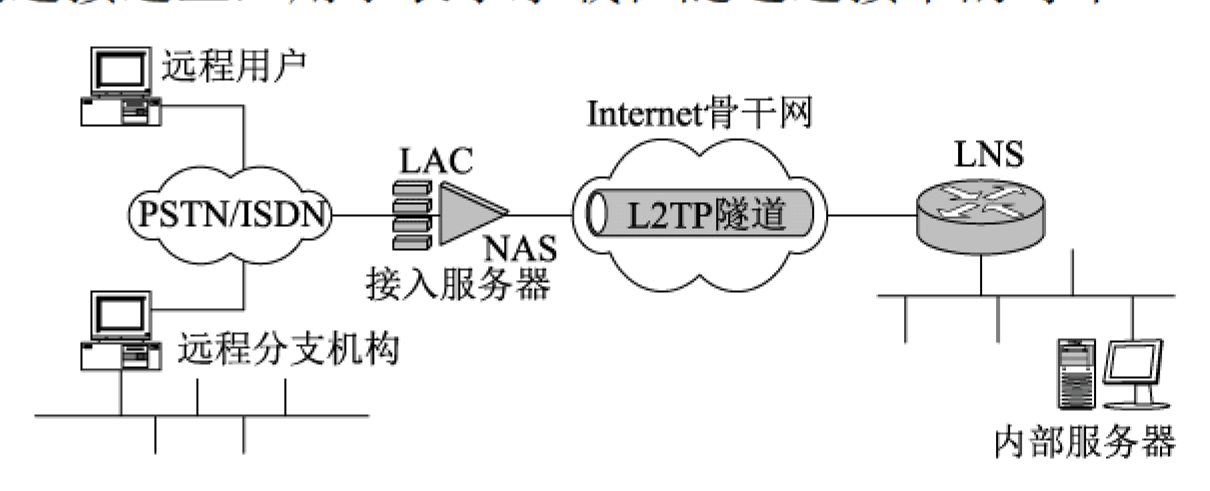


图 7.8 L2TP 的典型结构



7.2.4.3 IPSec

IPSec 协议不是一个单独的协议，它给出了应用于 IP 层上网络数据安全的一整套体系结构，包括网络认证协议(Authentication Header，AH)、封装安全载荷协议(Encapsulating Security Payload，ESP)、密钥管理协议(Internet Key Exchange，IKE)和用于网络认证及加密的一些算法等。IPSec 规定了如何在对等层之间选择安全协议，确定安全算法和密钥交换，向上提供了访问控制、数据源认证、数据加密等网络安全服务。

1. 网络认证协议

网络认证协议(Authentication Header，AH)为 IP 通信提供数据源认证、数据完整性和反重播保证，它能保护通信免受篡改，但不能防止窃听，适用于传输非机密数据。AH 的工作原理是在每一个数据包上添加一个身份验证报头，此报头包含一个带密钥的 Hash 散列，可以将其当作数字签名，但它不使用证书，此 Hash 散列在整个数据包中计算，因此对数据的任何更改将致使散列无效，这样就提供了完整性保护。但是 AH 不提供保密服务。IPSec 支持的认证算法有 HMAC-MD5 和 HMAC-SHA1。

2. 封装安全载荷协议

封装安全载荷协议(Encapsulating Security Payload，ESP)为 IP 数据包提供完整性检查、认证和加密，它提供机密性并可防止篡改。ESP 服务依据建立的安全关联(SA)是可选的，然而也有一些限制，它必须与完整性检查和认证一起进行。仅当它与完整性检查和认证一起时，重播(Replay)保护才是可选的。重播保护只能由接收方选择。

ESP 的加密服务是可选的，但如果启用加密，则也就同时选择了完整性检查和认证。因为如果仅使用加密，入侵者就可能伪造报文以发动密码分析攻击。

ESP 可以单独使用，也可以和 AH 结合使用。一般 ESP 不对整个数据包加密，而只加密 IP 包的有效载荷部分，不包括 IP 头。但在端对端的隧道通信中，ESP 需要对整个数据包加密。ESP 报头插在 IP 报头之后，TCP 或 UDP 等传输层协议报头之前。ESP 由 IP 协议号 50 标识。

3. 密钥管理协议

密钥管理协议(Internet Key Exchange，IKE)是 Internet 工程任务组(IETF)制定的安全关联标准法和密钥交换解决方案，它提供一种方法供两台计算机建立安全关联(Security Association，SA)。SA 对两台计算机之间的策略协议进行编码，指定它们将使用哪些算法和什么样的密钥长度，以及实际的密钥本身。IKE 主要完成两个任务：一是安全关联的集中化管理，减少连接时间；二是密钥的生成和管理。

4. 实现方式

IPSec 可以在端系统或者安全网关中实现；也可以在现有的 IP 实现中集成 IPSec，这种方法需要能够修改现有 IP 实现的源码；BIST(Bump in the Stack)实现方式是在已有的 IP 协议栈中实现 IPSec，使之存在于 IP 协议和网络驱动器之间；BITW(Bump in the Wire)实现方式是在外部的加密机中实现 IPSec，从而在两个路由器或两个主机之间形成安全隧道。

IPSec 的一个重要实现方式是基于 VPN 的加密机制，由 IPSec 构成的加密 IP 隧道提供不同介质和地域网间的安全透明连接。

7.2.4.4　安全套接层

安全套接层(Secure Socket Layer，SSL)是Netscape公司设计的主要用于Web的安全传输协议。这种协议在Web上获得了广泛的应用。

SSL是一个介于HTTP协议与TCP之间的一个可选层。当发送访问请求时，在SSL层，借助下层协议的信道安全协商出一份加密密钥，并用此密钥来加密HTTP请求；在TCP层，与服务器端口建立连接，传递SSL处理后的数据。接收端与此过程相反。这样，SSL在TCP之上建立了一个加密通道，通过这一层的数据经过了加密，因此可达到保密的效果。

SSL协议分为两部分：握手协议(Handshake Protocol，HP)和记录协议(Record Protocol，RP)。其中握手协议用来协商密钥，协议的大部分内容是通信双方如何利用它来安全地协商出一份密钥；记录协议则定义了传输的格式。

1. 握手协议

握手协议是SSL的客户端，也是TCP的客户端，在TCP连接建立之后，发出一个Clienthello来发起握手，这个消息中包含了客户端自己可实现的算法列表和其他一些需要的消息，SSL的服务器端会回应一个Serverhello，其中确定了通信所需要的算法，然后发过去自己的证书，里面包含了身份和自己的公钥。客户端在收到这个消息后会生成一个秘密消息，用SSL服务器的公钥加密后传过去，SSL服务器端用自己的私钥解密后，会话密钥协商成功，双方可以用同一份会话密钥进行通信。

例如，一个用户通过浏览器访问SSL的Web服务器的过程如下。

(1) 浏览器和服务器开始建立一次SSL握手：双方协商使用的加密算法；浏览器端验证Web服务器提交的证书；双方协商生成会话密钥。

(2) Web服务器向浏览器发送所请求的数据：Web服务器计算原始数据的散列值；用会话密钥加密散列值；将密文发送给浏览器。

(3) 浏览器接收处理并显示数据：用会话密钥解密得到原始数据和散列值；使用相同的散列函数计算散列值；比较收到的散列值和计算出的散列值，如果相同则显示数据。

2. 记录协议

SSL记录协议是一个可相对独立工作的协议，它定义了传输的格式，其报文包含长度、描述符和用户数据等内容。记录协议完成的工作包括信息传输、数据分段、可选择的数据压缩、提供信息鉴别码和加密。

SSL记录层从上层接收任意长的用户数据，然后进行合适的分段，之后再使用压缩状态信息来压缩和解压缩记录。记录的另一个功能是负载保护，就是加密和完整性保护。

3. 传输层安全性

IETF将SSL作了标准化，标准文献是RFC 2246，并将其称为传输层安全性(Transport Layer Security，TLS)。从技术上讲，TLS与SSL的差别非常微小。TLS提供了客户机与服务器之间的安全连接。TLS协议运行于TCP/IP之上，在高层协议(如HTTP)之下，因此它可以为高层协议数据提供机密性。安全连接所提供的信任、机密性和性能的级别各有不同，并且都取决于客户机和服务器的TLS配置。



7.2.4.5　Windows 平台的 VPN 配置

1. 创建 VPN 服务器

Windows Server 2003 中 VPN 服务被称为路由和远程访问，默认状态已经安装，只需对此服务进行必要的配置，使其生效即可。创建 VPN 服务器的步骤如下。

(1) 以管理员身份登录 Windows Server 2003，依次选择“开始”→“管理工具”→“配置您的服务器向导”命令，启动如图 7.9 所示的“配置您的服务器向导”对话框。

(2) 单击“下一步”按钮，在如图 7.10 所示的“预备步骤”界面中单击“下一步”按钮。

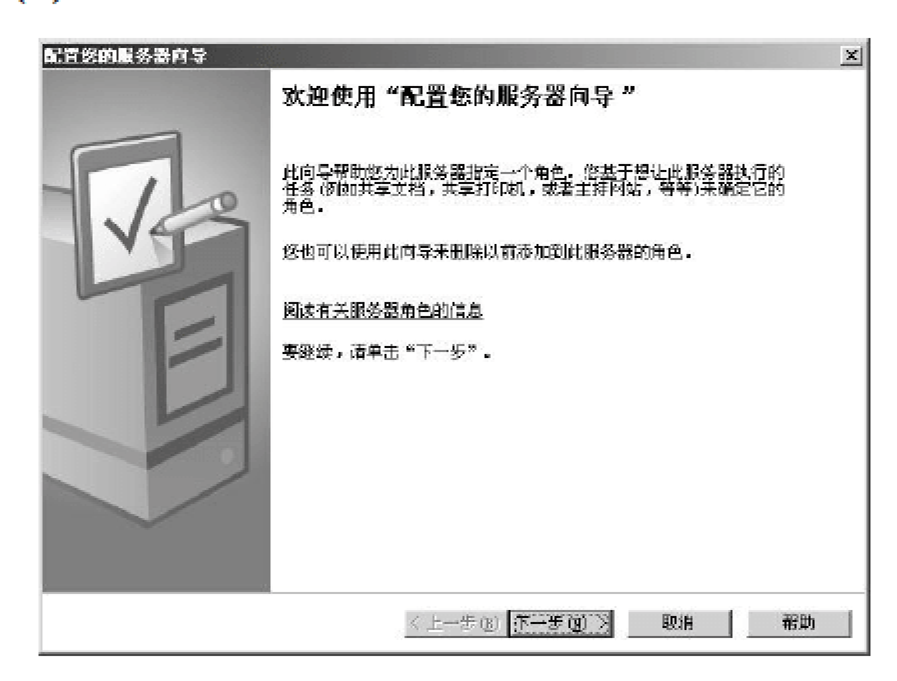


图 7.9　“配置您的服务器向导”对话框



图 7.10　“预备步骤”界面

(3) 在如图 7.11 所示的“服务器角色”界面中，选择“远程访问/VPN 服务器”选项，单击“下一步”按钮。

(4) 在如图 7.12 所示的“选择总结”界面中，单击“下一步”按钮。

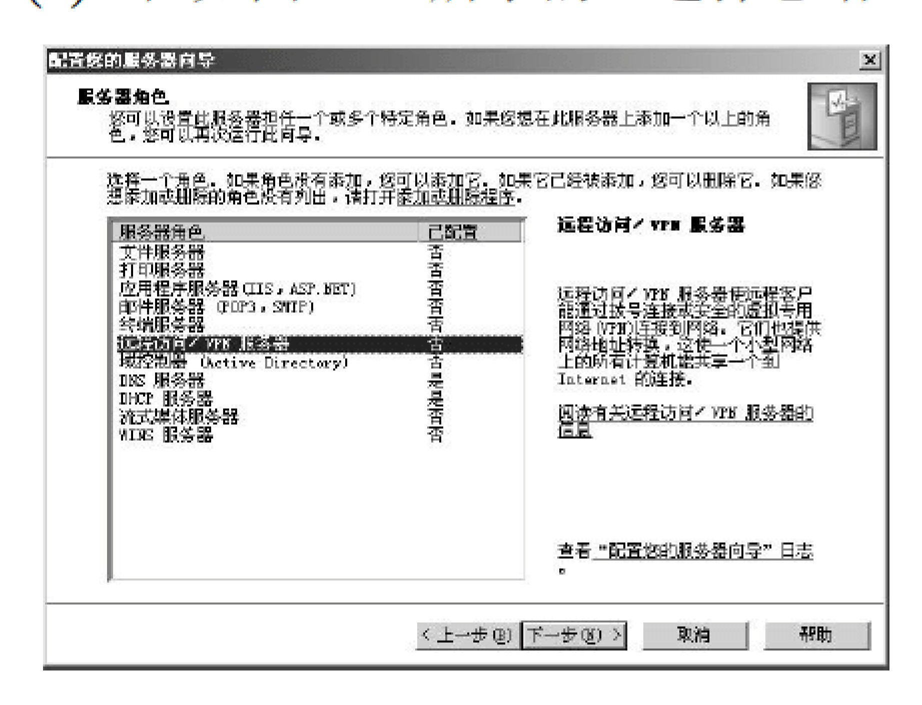


图 7.11　“服务器角色”界面

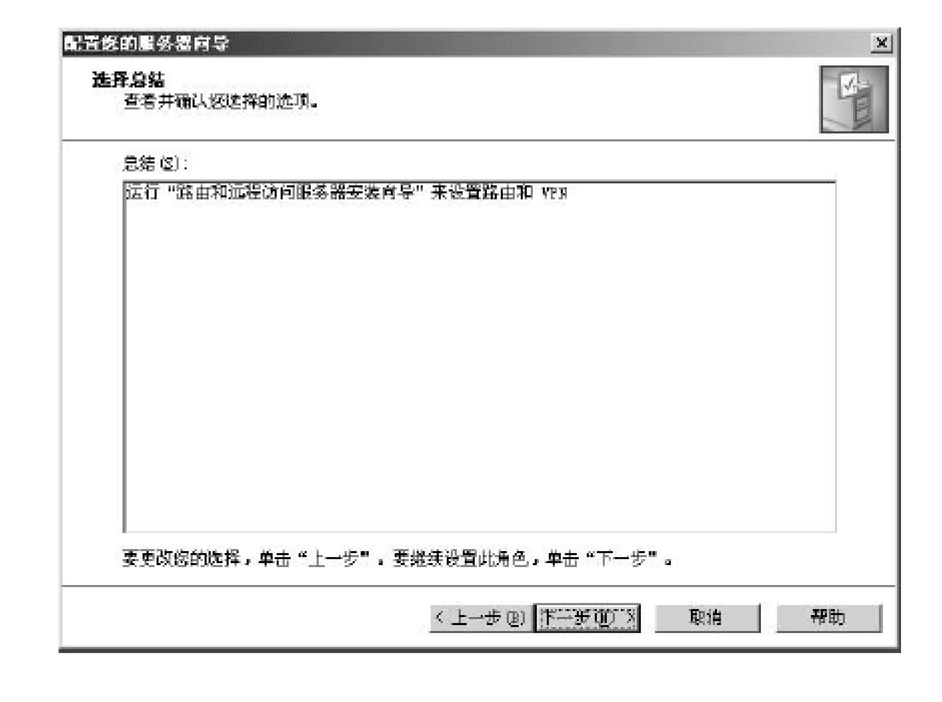


图 7.12　“选择总结”界面

(5) 系统启动“路由和远程访问服务器安装向导”，如图 7.13 所示，单击“下一步”按钮。

(6) 在如图 7.14 所示的“配置”界面中，选中“远程访问(拨号或 VPN)”单选按钮，然后单击“下一步”按钮。

(7) 在如图 7.15 所示的“远程访问”界面中，选中 VPN 复选框，单击“下一步”按钮。

(8) 接下来，向导将列出系统上所有的网络接口。选择与 Internet 相连的网络接口，如图 7.16 所示，然后单击“下一步”按钮。

(9) 在如图 7.17 所示的“IP 地址指定”界面中，需要选择如何为远程客户端分配 IP 地址。如果局域网中配置了 DHCP 服务器，则可由 DHCP 服务器从其地址池中为远程客户分

配 IP 地址，否则需要手工设置一个 IP 地址范围，用于分配给远程客户端使用。这里我们选中“自动”单选按钮，单击“下一步”按钮。

(10) 在如图 7.18 所示的“管理多个远程访问服务器”界面中，选中“否，使用路由和远程访问来对连接请求进行身份验证”单选按钮，单击“下一步”按钮。

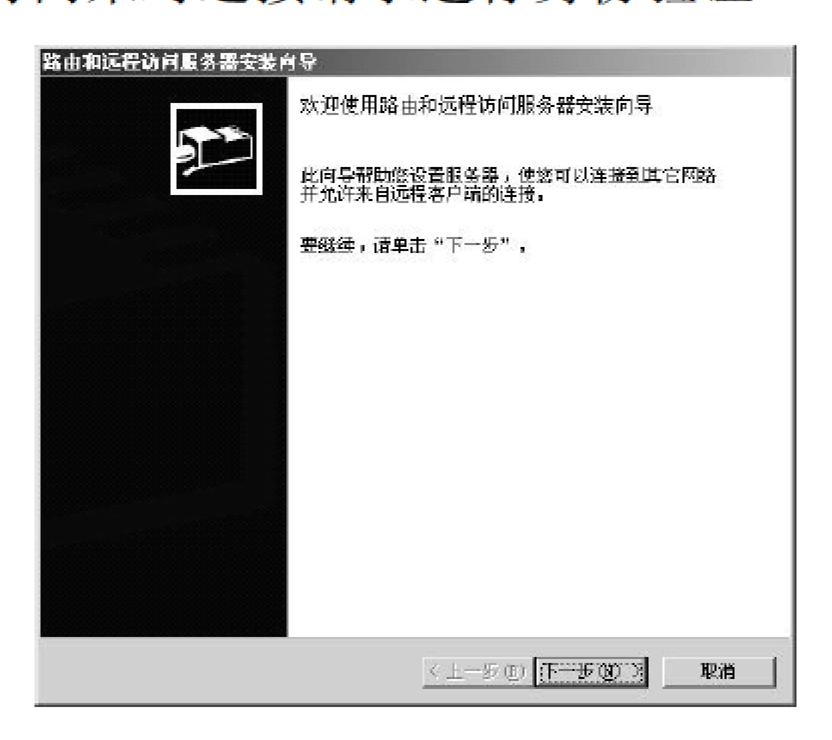


图 7.13　路由和远程访问服务器安装向导

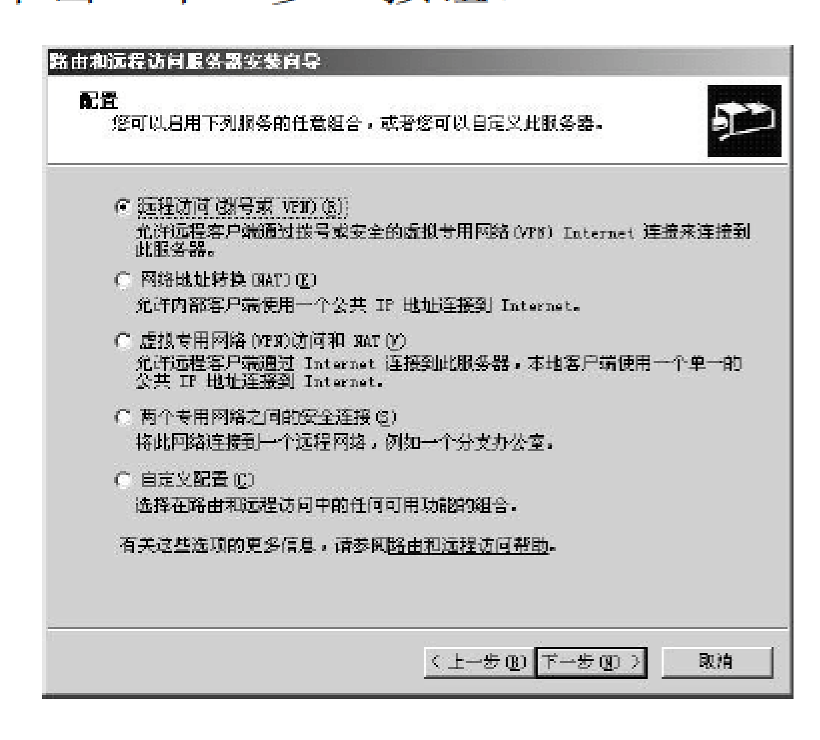


图 7.14　“配置”界面

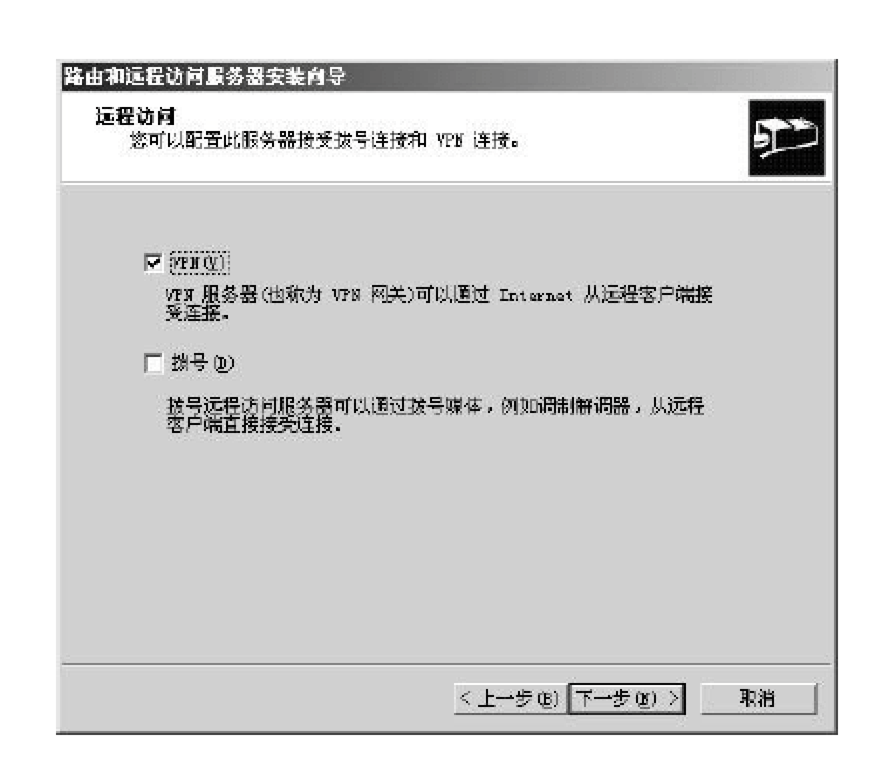


图 7.15　“远程访问”界面

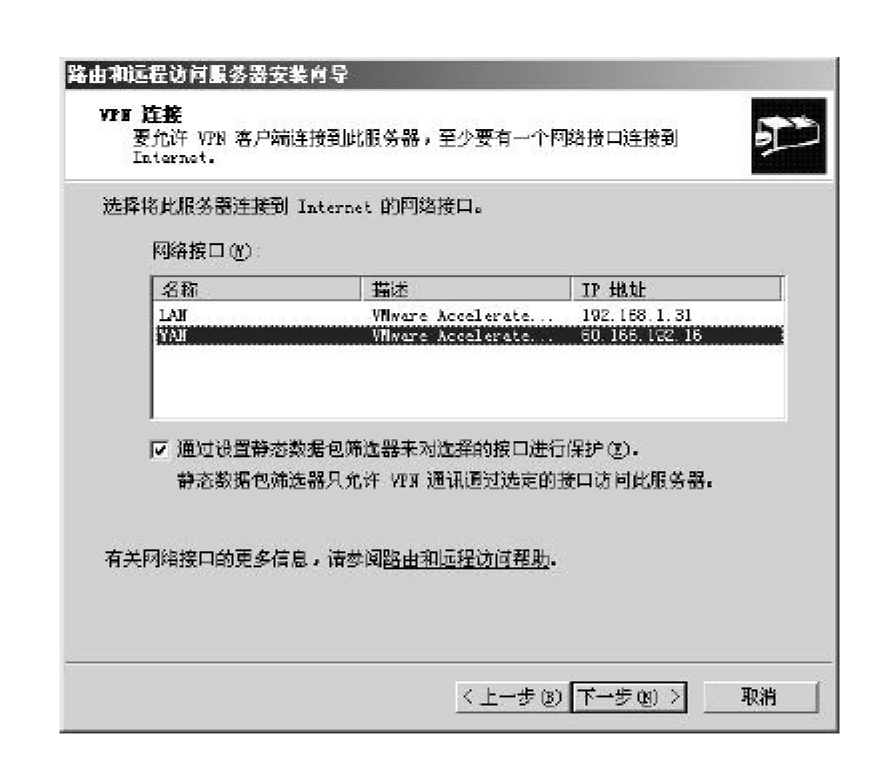


图 7.16　选择网络接口



图 7.17　“IP 地址指定”界面

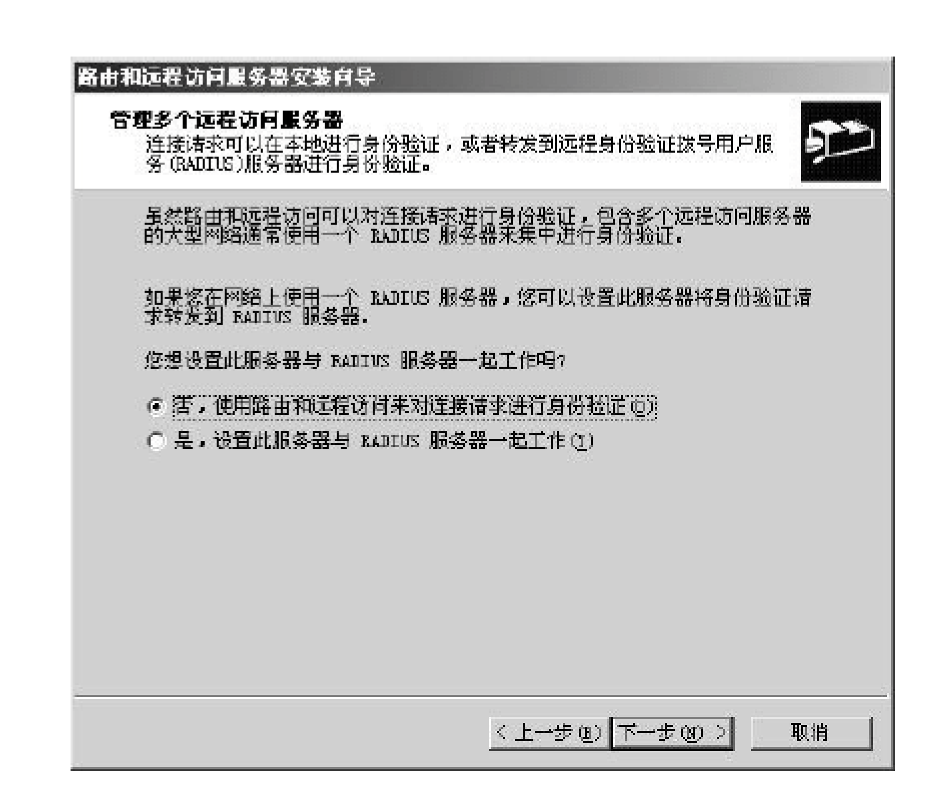


图 7.18　“管理多个远程访问服务器”界面

(11) 系统将开始配置 VPN 服务，配置完成后，将显示如图 7.19 所示的界面，单击“完成”按钮。

(12) 在如图 7.20 所示的“此服务器现在是远程访问/VPN 服务器”界面中，单击“完成”按钮。



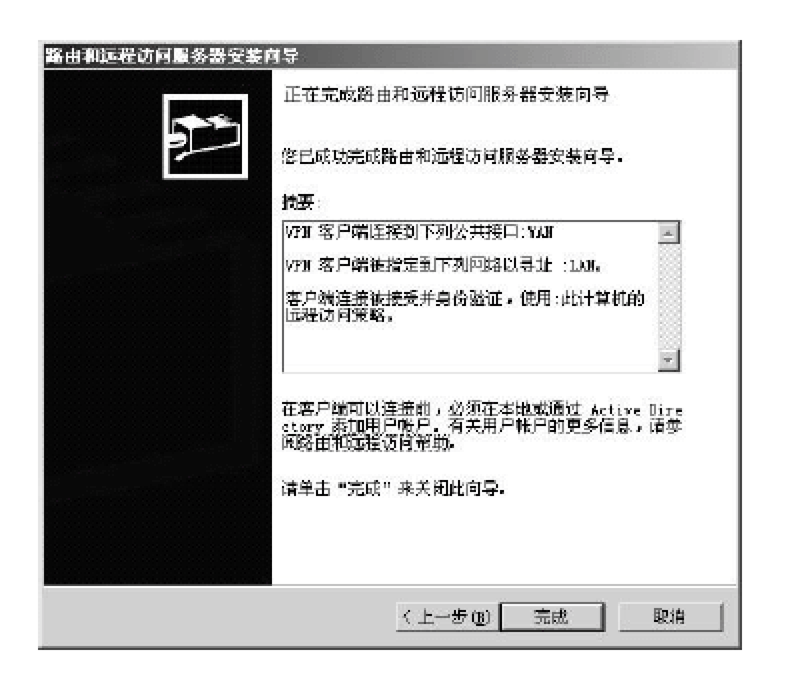


图 7.19　“正在完成路由和远程访问服务器安装向导”界面

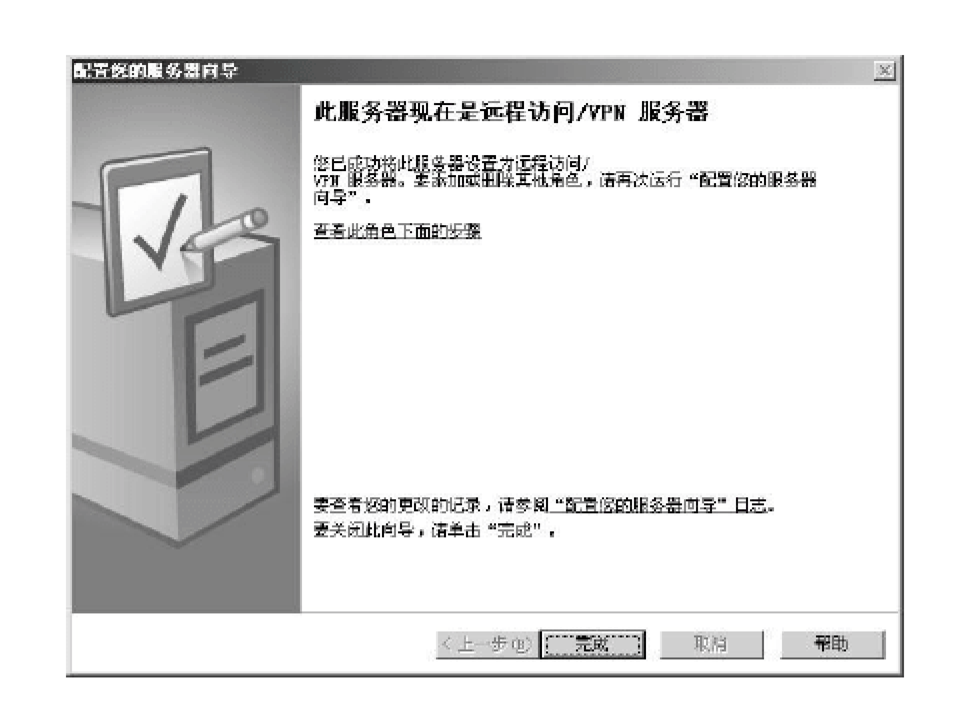


图 7.20　VPN 服务器配置完成

VPN 服务器创建完成后，用户可通过依次选择“开始”→“管理工具”→“路由和远程访问”命令，打开“路由和远程访问”控制台，如图 7.21 所示。在此，用户可对 VPN 服务器进行一些管理和参数的设置。当然，此时即使不做任何额外的设置，VPN 服务器也能正常工作。

2. 添加权限账户

拨入 VPN 服务器需要有一个账号，默认情况下，用户远程访问的权限是被禁止的。

要允许某个用户拥有访问 VPN 服务器的权限，需要在用户的属性对话框中切换到“拨入”选项卡，在“远程访问权限(拨入或 VPN)”选项组中选中“允许访问”单选按钮，以允许该用户通过 VPN 拨入服务器，如图 7.22 所示。

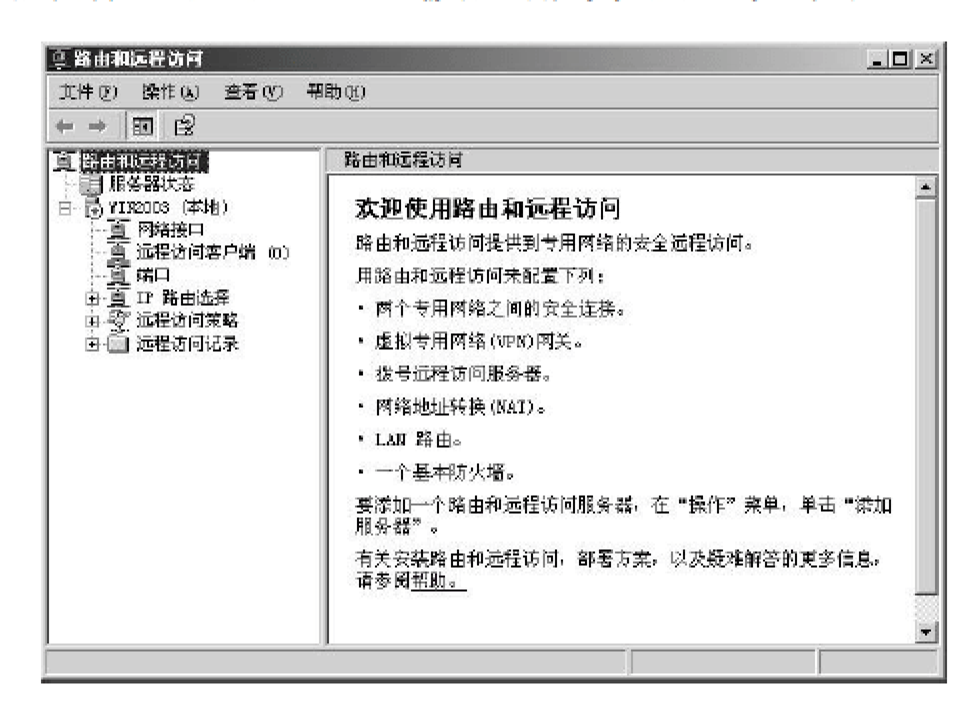


图 7.21　“路由和远程访问”控制台

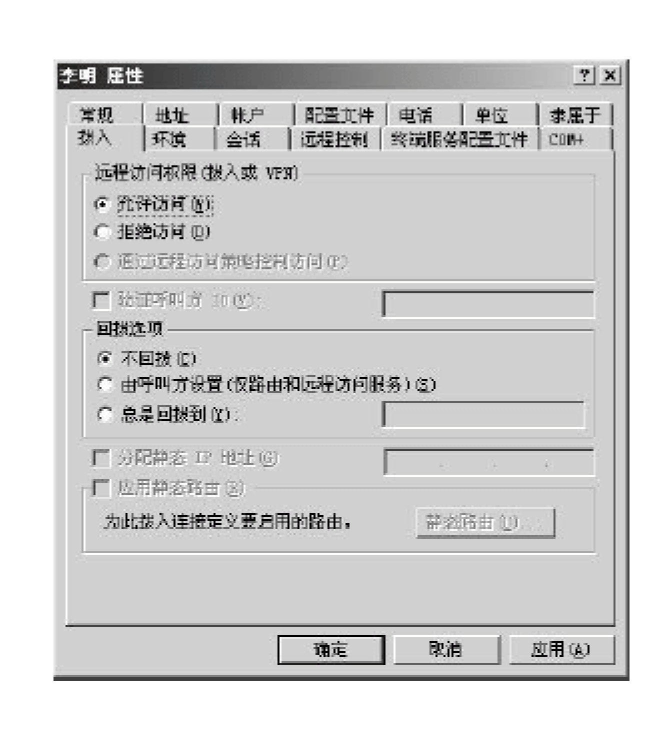


图 7.22　“拨入”选项卡

3. 连接 VPN 服务器

在 Windows XP 上连接 VPN 的操作步骤如下。

(1) 打开“控制面板”窗口，如图 7.23 所示，单击“网络和 Internet 连接”图标。

(2) 在如图 7.24 所示的“网络和 Internet 连接”窗口中，选择“创建一个到您的工作位置的网络连接”选项。

(3) 在如图 7.25 所示的“网络连接”界面中选中“虚拟专用网络连接”单选按钮，单击“下一步”按钮。

(4) 在如图 7.26 所示的“连接名”界面中输入连接名称，如公司的名称，单击“下一步”按钮。



图 7.23 “控制面板”窗口



图 7.24 “网络和 Internet 连接”窗口



图 7.25 “网络连接”界面



图 7.26 “连接名”界面

(5) 在如图 7.27 所示的“VPN 服务器选择”界面中，输入 VPN 服务器的主机名或者 IP 地址，例如，vpn.example.com，单击“下一步”按钮。

(6) 在如图 7.28 所示的“正在完成新建连接向导”界面中，单击“完成”按钮。

VPN 连接创建完成后，双击桌面上的“VPN 连接”图标，在弹出的对话框中输入用户名和密码，如图 7.29 所示，然后单击“连接”按钮，就可以与 VPN 服务器连接上了。



图 7.27 “VPN 服务器选择”界面

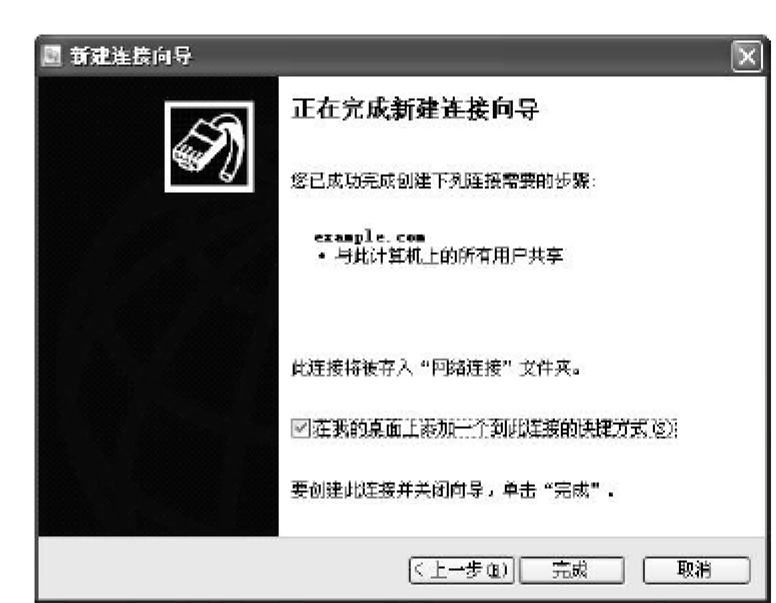


图 7.28 “正在完成新建连接向导”界面

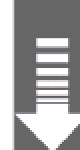


图 7.29 连接 VPN

7.2.5 应用层安全协议

7.2.5.1 安全超文本传输协议

安全超文本传输协议(Secure Hypertext Transfer Protocol，S-HTTP)是一种结合 HTTP 而设计的消息安全通信协议。S-HTTP 的设计基于与 HTTP 信息样板共存并易于与 HTTP 应用



程序相整合。

S-HTTP 协议为 HTTP 客户机和服务器提供了多种安全机制，这些安全服务选项是适用于万维网上各类用户的，还为客户机和服务器提供了对称能力(及时处理请求和回复，以及两者的参数选择)，同时维持 HTTP 的通信模型和实时特征。

S-HTTP 不需要客户方的公用密钥证明(或公用密钥)，但它支持对称密钥的操作模式。这点很重要，因为这意味着在没有要求用户个人建立公用密钥的情况下，会自发地发生私人交易。它支持端对端安全传输，客户机可能首先启动安全传输(使用报头的信息)，用来支持加密技术。

在语法上，S-HTTP 报文与 HTTP 相同，由请求或状态行组成，后面是信头和主体。请求报文的格式由请求行、通用信息头、请求头、实体头、信息主体组成。响应报文由响应行、通用信息头、响应头、实体头、信息主体组成。

7.2.5.2　邮件加密软件

邮件加密软件(Pretty Good Privacy，PGP)是一个基于 RSA 公匙加密体系的邮件加密软件。用户可以用它对邮件保密以防止非授权者阅读，还能对邮件加上数字签名，从而使收信人可以确信邮件是原发送方所发来的。它让用户可以安全地和从未见过的另一方通信，事先并不需要任何保密的渠道来传递密钥。PGP 也可以用来加密文件，因此 PGP 成为流行的公钥加密软件包。

PGP 采用了审慎的密钥管理，是一种 RSA 和传统加密的杂合算法，用于数字签名的邮件文摘算法、加密前压缩等方法。PGP 用一个 128 位的二进制数作为邮件文摘，发送方用自己的私钥将上述的 128 位的特征值加密，附加在邮件后，再用接收方的公钥将整个邮件加密。密文被接收方收到以后，接收方用自己的私钥将邮件解密，得到原文和签名，接收方的 PGP 也从原文计算出一个 128 位的特征值来与用发送方的公钥解密签名所得到的数比较，如果符合就说明这份邮件确实是发送方寄来的。这样两个安全性要求都得到了满足。

7.2.5.3　S/MIME

S/MIME(Security/Multipurpose Internet Mail Extensions)是 RSA 数据安全公司开发的软件。S/MIME 提供的安全服务有报文完整性验证、数字签名和数据加密。S/MIME 可以添加在邮件系统的用户代理中，用于提供安全的电子邮件传输服务，也可以加入其他传输机制中，安全地传输任何 MIME 报文，甚至可以添加到自动报文传输代理中，在 Internet 中安全地传送由软件生成的 FAX 报文。

S/MIME 的安全功能基于加密信息语法标准 PKCS#7(RFC 2315)和 X.509v3 证书，密钥长度是动态可变的，具有很高的灵活性。

7.2.5.4　安全的电子交易

安全的电子交易(Secure Electronic Transaction，SET)用于电子商务的行业规范，是一种应用在 Internet 上、以信用卡为基础的电子付款系统规范，目的就是保证网络交易的安全。SET 主要使用“电子认证”技术作为保密电子交易安全进行的基础，其认证过程使用 RSA 和 DES 算法。

SET 提供以下 3 种服务。

- 在交易涉及的对方之间提供安全信道。
- 使用 X.509 数字证书实现安全的电子交易。
- 保证信息的机密性。

SET 交易发生的先决条件是：每一个持卡人(客户)必须拥有唯一的电子(数字)证 书，且由客户确定口令，并用这个口令对数字证书、私钥、信用卡号码以及其他信息进行加密存储。这些与符合 SET 协议的软件一起组成了一个 SET“电子钱包”。

7.2.5.5 Kerberos 系统

Kerberos 是 MIT 在 1980 年为 Athena 计划的认证服务而开发的、一种基于密钥分发和可信中继认证方法的鉴别服务系统。

Kerberos 系统是一种基于密钥分配中心(KDC)概念的分布式鉴别服务系统，它可以在不安全的网络环境中为用户对远程服务器的访问提供自动鉴别、数据安全性和完整性服务，以及密钥管理。

1. Kerberos 鉴别

Kerberos 要求用户使用其用户名和口令作为自己的标识，而客户端与 KDC 服务器之间的交互则使用由对应的用户名和口令所生成的会话密钥。会话密钥由每个用户与 KDC 服务器共享。当用户登录后，便从 KDC 处获得这个会话密钥，用于与对应的服务器交互。

当用户需要和其他用户通信时，需要从服务器端获得 TGT(Ticket-Granting Ticket)，然后再用 TGT 向 KDC 服务器申请与需要通信的一方交互的会话密钥，接收到这个密钥后，就可以与对应用户通信了。

A 与 B 建立通信的整个过程如下。

K_a：A 与 KDC 会话密钥。

K_b：B 与 KDC 会话密钥。

K_{ab}：A 与 B 会话密钥。

S_a,S：时间标记，用以防止中途报文被截获再重发。

(1) A 与 KDC 交互。

第一步：A 登录系统，向 KDC 请求 TGT。

第二步：KDC 向 A 发送用 K_a 加密的 $K_a(S_a,TGT)$，其中 S_a 是时间标识。

第三步：A 用自己的 K_a 解密出 S_a，TGT 将其返回给 KDC 以证明自己是 A。

第四步：KDC 认证 A 的身份后，产生 A 与 B 的会话密钥 K_{ab}，并用与 B 的会话密钥 K_b 加密 K_{ab} 和对 A 的信任信息，即 K_b(trust-A, K_{ab})，把整个报文标记上时标一起发送给 A。

(2) A 接收到密钥信号后，与 B 建立交互通信。

第一步：A 向 B 发送从 KDC 得到的 K_b(trust-A, K_{ab})，以及 $K_{ab}(S)$，其中 S 为时间标识。

第二步：B 用自己的 K_b 解密 A 发来的内容，得到 trust-A 和 K_{ab}，从而确认 A 的身份，再用 K_{ab} 解密时标 S，向 A 传送 $K_{ab}(S+1)$。

第三步：A 用 K_{ab} 解密出 $S+1$，从而证明对方有 K_b，确认了 B 的身份。

(3) 此后，双方开始用 K_{ab} 交互。



2. Kerberos 安全机制

在 Kerberos 系统中使用对称密钥体制中的 CBC 方式的一个变形 PCBC(Plaintext Cliper Block Chaining)来实现数据的加密和完整性保护。效果是，加密链中间部分被破坏，那么从此处到最后所有报文都要受到影响。

为了防止中途报文被截获再重发，通信双方还要提供时间标识，再根据对方发来的时标判断这个请求是否是攻击者截获的旧信息。

7.2.6　防火墙的配置

7.2.6.1　防火墙介绍

任何企业安全策略的一个主要部分都是实现和维护防火墙，因此防火墙在网络安全的实现中扮演着重要的角色。防火墙通常位于企业网络的边缘，这使得内部网络与 Internet 或者其他外部网络互相隔离，并限制网络互访，从而保护企业内部网络。设置防火墙的目的都是在内部网与外部网之间设立唯一的通道，简化网络的安全管理。

防火墙通过监测、限制、更改跨越防火墙的数据流，尽可能地对外部屏蔽网络内部的信息、结构和运行状况，以此来实现网络的安全保护。

防火墙的基本类型包括以下几种。

- 包过滤型防火墙：通过访问控制表，检查数据流中每个数据包的源地址、目的地址、所用的端口号、协议状态等因素，来确定是否允许该数据包通过。
- 应用网关防火墙：它工作在 OSL 模型的应用层，能针对特别的网络应用协议制定数据过滤规则。
- 代理服务器防火墙：它工作在 OSI 模型的应用层，主要使用代理技术来阻断内部网络和外部网络之间的通信，达到隐藏内部网络的目的。
- 状态检测防火墙：也叫自适应防火墙或动态包过滤防火墙。这种防火墙能通过状态检测技术动态记录、维护各个连接的协议状态，并且在网络层和 IP 之间插入一个检查模块，对 IP 包的信息进行分析检测，以决定是否允许通过。
- 自适应代理防火墙：根据用户的安全策略，动态适应传输中的分组流量。它整合了动态包过滤防火墙技术和应用代理技术，本质上是状态检测防火墙。

在众多的企业级主流防火墙中，Cisco PIX 防火墙是所有同类产品中性能最好的一种。Cisco PIX 系列防火墙目前有 5 种型号：PIX506、PIX515、PIX520、PIX525、PIX535。这里仅以 PIX 525 为例介绍防火墙的配置。

7.2.6.2　防火墙的物理特性

在配置 PIX 防火墙之前，先来介绍一下防火墙的物理特性。防火墙通常至少具有 3 个接口，但许多早期的防火墙只有 2 个接口。当使用具有 3 个接口的防火墙时，会产生至少 3 个网络，它们的描述如下。

1. 内部区域

内部区域(内网)通常是指企业内部网络或者企业内部网络的一部分。它是互联网(Interconnection Network)的信任区域，即受到了防火墙的保护。

2. 外部区域

外部区域(外网)通常指 Internet 或者非企业内部网络。它是互联网中不被信任的区域，当外部区域想要访问内部区域的主机和服务时，通过设置防火墙就可以实现有限制的访问。

3. 非军事区

非军事区(DMZ)是一个隔离的网络或几个网络。位于非军事区中的主机或服务器被称为堡垒主机。一般在非军事区内可以放置 Web 服务器和 Mail 服务器等。非军事区对于外部用户通常是可以访问的，这种方式允许外部用户访问企业的公开信息，但不允许他们访问企业内部网络。

7.2.6.3 防火墙的管理模式

PIX 防火墙提供以下 4 种管理访问模式。

1. 非特权模式

PIX 防火墙开机自检后，就是处于非特权模式。此时，系统显示为 pixfirewall> 。

2. 特权模式

输入 enable 进入特权模式，可以改变当前配置。此时，系统显示为 pixfirewall# 。

3. 配置模式

输入 configure terminal 进入配置模式，绝大部分的系统配置都在这里进行。此时，系统显示为 pixfirewall(config)# 。

4. 监视模式

PIX 防火墙在开机或重启过程中，按住 Escape 键或发送一个“Break”字符，可以进入监视模式。在这里可以更新操作系统映像和口令恢复。此时，系统显示为 monitor>。

7.2.6.4 PIX 防火墙的基本命令

下面介绍配置 PIX 防火墙的 6 个基本命令：nameif、interface、ip address、nat、global 和 route。

1. nameif

nameif 命令用于配置防火墙接口的名字，并指定安全级别。

```
Pix525(config)#nameif ethernet0 outside security 0
Pix525(config)#nameif ethernet1 inside security 100
Pix525(config)#nameif dmz security 50
```

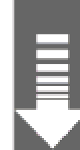
提示：在默认配置中，以太网 0 被命名为外部接口(outside)，安全级别是 0；以太网 1 被命名为内部接口(inside)，安全级别是 100。安全级别的取值范围为 1～99，数字越大，安全级别越高。若添加新的接口，语句如下。

```
Pix525(config)#nameif pix/intf3 security 40 (安全级别任取)
```

2. interface

interface 命令用于配置以太网参数。

```
Pix525(config)#interface ethernet0 auto(auto 选项表明系统自适应网卡类型)
```



```
Pix525(config)#interface ethernet1 100full(100full 选项表示 100Mb/s 以太网全双工通信)
Pix525(config)#interface ethernet1 100full shutdown (shutdown 选项表示关闭这个接口，若启用接口则去掉 shutdown)
```

3. ip address

ip address 命令用于配置内外网卡的 IP 地址。

```
Pix525(config)#ip address outside 61.144.51.42 255.255.255.248
Pix525(config)#ip address inside 192.168.0.1 255.255.255.0
```

提示：Pix525 防火墙在外网的 IP 地址是 61.144.51.42，内网 IP 地址是 192.168.0.1。

4. nat

nat 命令用于指定要进行转换的内部地址。

网络地址翻译(nat)的作用是将内网的私有 IP 转换为外网的公有 IP。nat 命令总是与 global 命令一起使用，这是因为 nat 命令可以指定一台主机或一段范围的主机访问外网，访问外网时需要利用 global 所指定的地址池进行对外访问。

nat 命令的配置语法如下。

```
nat (if_name) nat_id local_ip
```

其中，(if_name)表示内网接口名字；nat_id 用来标识全局地址池，使它与其相应的 global 命令相匹配；local_ip 表示内网被分配的 IP 地址。例如 0.0.0.0 表示内网所有主机可以对外访问。

例 1　Pix525(config)#nat (inside) 1 0 0

表示启用 nat，内网的所有主机都可以访问外网，用 0 可以代表 0.0.0.0。

例 2　Pix525(config)#nat (inside) 1 172.17.5.0 255.255.0.0

表示只有 172.17.5.0 这个网段内的主机可以访问外网。

5. global

global 命令用于指定外部地址范围。

global 命令把内网的 IP 地址翻译成外网的 IP 地址或一段地址范围。

global 命令的配置语法如下。

```
global (if_name) nat_id ip_address-ip_address
```

其中，(if_name)表示外网接口名字；nat_id 用来标识全局地址池，使它与其相应的 nat 命令相匹配；ip_address-ip_address 表示翻译后的单个 IP 地址或一段 IP 地址的范围。

例 3　Pix525(config)#global (outside) 1 61.144.51.42-61.144.51.48

表示内网的主机通过 PIX 防火墙要访问外网时，PIX 防火墙将使用 61.144.51.42-61.144.51.48 这段 IP 地址池为要访问外网的主机分配一个全局 IP 地址。

例 4　Pix525(config)#global (outside) 1 61.144.51.42

表示内网要访问外网时，PIX 防火墙将为访问外网的所有主机统一使用 61.144.51.42 这个单一 IP 地址。

例 5　Pix525(config)#no global (outside) 1 61.144.51.42

表示删除这个全局表项。

6. route

route 命令用于设置指向内网和外网的静态路由。

route 命令的配置语法如下。

```
route (if_name) 0 0 gateway_ip  number
```

其中，(if_name)表示接口名字，例如 inside 和 outside；gateway_ip 表示网关路由器的 IP 地址；number 表示到 gateway_ip 的跳数，通常默认是 1。

例 6　Pix525(config)#route outside 0 0 61.144.51.168 1

表示一条指向边界路由器(IP 地址为 61.144.51.168)的默认路由。

例 7　Pix525(config)#route inside 10.1.1.0 255.255.255.0 172.17.0.1 1
　　　Pix525(config)#route inside 10.2.0.0 255.255.0.0 172.17.0.1 1

如果内部网络只有一个网段，按照例 6 那样设置一条默认路由即可；如果内部存在多个网络，就需要配置一条以上的静态路由。例 7 表示创建了一条到网络 10.1.1.0 的静态路由，静态路由的下一条路由器 IP 地址是 172.17.0.1。

7.2.6.5　PIX 防火墙高级配置

1. 配置静态 IP 地址翻译命令——static

如果从外网发起一个会话，会话的目的地址是一个内网的 IP 地址，static 就把内部地址翻译成一个指定的全局地址，允许这个会话建立。

static 命令的配置语法如下。

```
static  (internal_if_name,  external_if_name)  outside_ip_address  inside_
ip_address
```

其中，internal_if_name 表示内部网络接口，安全级别较高，如 inside。

external_if_name 为外部网络接口，安全级别较低，如 outside 等。

outside_ip_address 为正在访问的较低安全级别接口上的 IP 地址。

inside_ ip_address 为内部网络的本地 IP 地址。

例 8　Pix525(config)#static (inside, outside) 61.144.51.62 192.168.0.8

表示 IP 地址为 192.168.0.8 的主机，对于通过 PIX 防火墙建立的每个会话，都被翻译成 61.144.51.62 这个全局地址。也可以理解成 static 命令创建了内部 IP 地址 192.168.0.8 和外部 IP 地址 61.144.51.62 之间的静态映射。

例 9　Pix525(config)#static (inside, outside) 192.168.0.2 10.0.1.3

表示创建了内部 IP 地址 192.168.0.2 和外部 IP 地址 10.0.1.3 之间的静态映射。

例 10　Pix525(config)#static (dmz, outside) 211.48.17.2 172.17.10.8

表示创建了 DMZ 的 IP 地址 211.48.17.2 和外部 IP 地址 172.17.10.8 之间的静态映射。

以上几个例子说明使用 static 命令可以让我们为一个特定的内部 IP 地址设置一个永久的全局 IP 地址。这样就能够为具有较低安全级别的指定接口创建一个入口，使它们可以进入具有较高安全级别的指定接口。



2. 管道命令——conduit

前面讲过使用 static 命令可以在一个本地 IP 地址和一个全局 IP 地址之间创建一个静态映射，但从外部到内部接口的连接仍然会被 PIX 防火墙的自适应安全算法(ASA)阻挡，而 conduit 命令用来允许数据流从具有较低安全级别的接口流向具有较高安全级别的接口，例如允许从外部到 DMZ 或内部接口的会话。对于向内部接口的连接，static 和 conduit 命令将一起使用，来指定会话的建立。

conduit 命令的配置语法如下。

```
conduit permit | deny global_ip port<-port> protocol foreign_ip
```

其中，permit | deny 表示允许或拒绝访问。

global_ip 指的是先前由 global 或 static 命令定义的全局 IP 地址，如果 global_ip 为 0，就用 any 代替 0；如果 global_ip 是一台主机，就用 host 命令参数。

port 指的是服务所作用的端口，例如 WWW 使用 80，SMTP 使用 25 等，我们可以通过服务名称或端口数字来指定端口。

protocol 指的是连接协议，比如 TCP、UDP 和 ICMP 等。

foreign_ip 表示可访问 global_ip 的外部 IP。对于任意主机，可以用 any 表示。如果 foreign_ip 是一台主机，就用 host 命令参数。

例 11　Pix525(config)#conduit permit tcp host 192.168.0.8 eq www any

这个例子表示允许任何外部主机对全局地址为 192.168.0.8 的这台主机进行 http 访问。其中使用 eq 和一个端口来允许或拒绝对这个端口的访问。eq www 就是指允许或拒绝只对 www 的访问。

例 12　Pix525(config)#conduit deny tcp any eq ftp host 61.144.51.89

表示不允许外部主机 61.144.51.89 对任何全局地址进行 ftp 访问。

例 13　Pix525(config)#conduit permit icmp any any

表示允许 icmp 消息向内部和外部通过。

例 14　Pix525(config)#static (inside, outside) 61.144.51.62 192.168.0.3
Pix525(config)#conduit permit tcp host 61.144.51.62 eq www any

这个例子说明了 static 和 conduit 的关系。192.168.0.3 在内网是一台 Web 服务器，现在希望外网的用户能够通过 PIX 防火墙得到 Web 服务，所以先做 static 静态映射：192.168.0.3→61.144.51.62(全局)。然后利用 conduit 命令允许任何外部主机对全局地址 61.144.51.62 进行 http 访问。

3. 配置 fixup 协议

fixup 命令的作用是启用、禁止、改变一个服务或协议通过 PIX 防火墙。由 fixup 命令指定的端口是 PIX 防火墙要侦听的服务。

例 15　Pix525(config)#fixup protocol ftp 21

表示启用 ftp 协议，并指定 ftp 的端口号为 21。

例 16　Pix525(config)#fixup protocol http 80
Pix525(config)#fixup protocol http 1080

表示为 http 协议指定 80 和 1080 两个端口。

例 17 Pix525(config)#no fixup protocol smtp 80

表示禁用 smtp 协议。

4. 设置 telnet

telnet 有一个版本的变化，在 PIX OS 5.0(PIX 操作系统的版本号)之前，只能从内部网络上的主机通过 telnet 命令访问 PIX。在 PIX OS 5.0 及后续版本中，可以在所有的接口上启用 telnet 命令来访问 PIX。当从外部接口访问 PIX 防火墙时，telnet 数据流需要用 IPsec 提供保护，也就是说，用户必须配置 PIX 来建立一条到另外一台 PIX 路由器或 VPN 客户端的 IPSec 隧道。另外就是在 PIX 上配置 SSH，然后用 SSH 客户端从外部通过 telnet 命令访问 PIX 防火墙。PIX 支持 SSH1 和 SSH2，不过 SSH1 是免费软件，SSH2 是商业软件。相比之下，Cisco 路由器的 telnet 就做得不怎么样了。

telnet 命令的配置语法如下。

```
telnet local_ip
```

其中，local_ip 表示被授权通过 telnet 访问到 PIX 的 IP 地址。如果不设此项，PIX 的配置方式只能由 console 进行。

7.2.7 入侵检测

入侵检测是指监视或者在可能情况下，阻止入侵者试图控制自己的系统或者网络资源的安全保护机制。入侵检测通过监视受保护系统的状态和活动，采用异常检测或误用检测的方式，发现非授权的或恶意的系统及网络行为，为防范入侵行为提供有效手段。它基于非法行为和合法行为是可分的，即可以通过提取行为的模式特征来分析判断该行为的性质。

7.2.7.1 入侵检测系统的构成

美国国防部高级研究计划局(DARPA)提出的公共入侵检测框架(CIDF)由 4 个模块组成：事件产生器、事件分析器、事件数据库和响应单元，如图 7.30 所示。

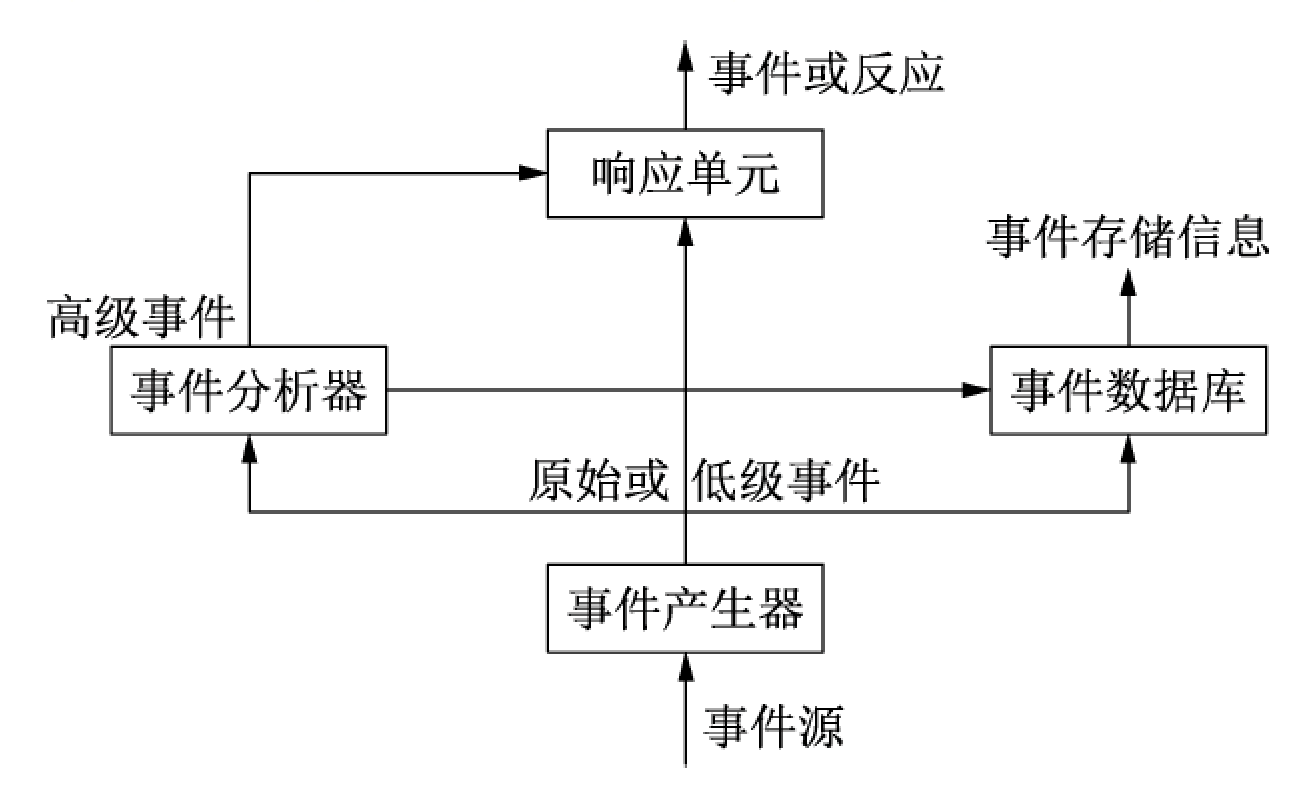


图 7.30 CIDF 体系结构

7.2.7.2 入侵检测系统

入侵检测系统(Intrusion Detection System，IDS)是一类专门面向网络入侵检测的网络安全检测系统，而且正在成为网络安全检测系统的主要内容。其基本功能包括：检测出正在

发生的攻击活动；发现攻击活动的范围和后果；诊断并发现攻击者的入侵方式和入侵地点，并给出解决建议；收集并记录入侵活动的证据。IDS 系统不仅针对外部入侵者，而且还可以对网络内部用户的行为进行监控，防止出现内部的攻击者。

IDS 系统的服务功能有：异常检测、滥用检测和攻击警告。

- 异常检测，是分析系统的行为，事先通过统计方法建立网络正常行为模型，根据当前行为是否符合模型来判断是否是异常行为。其目的是发现构成入侵的安全事件的集合在实践上的相关性，从而对未来发生的事件进行预测。系统具有修改和调整模型的能力，通过自我学习发现新的攻击类别和方式，但在实现上困难较大。
- 滥用检测，相当于防病毒软件中病毒的特征比对，它从检测到的数据中寻找已知的安全知识匹配，并根据预定政策报警。这类 IDS 的关键在于定义各种攻击的行为特征，对于已知攻击，发现是准确及时的，但是需要及时更新知识库中的安全知识，否则无法识别新的攻击。
- 攻击警告，监测入侵者入侵系统后会经常考虑触动的对象，如系统的账户管理数据库等，如果这些目标出现异常，则发出报警。攻击警告依赖于系统管理员对网络行为的正确理解程度和制定合适的报警政策。

7.2.7.3　入侵检测系统的部署

目前的网络都是交换式的拓扑结构，因此一般选择在尽可能接近受保护资源的地方部署入侵检测系统。这些位置通常如下。

- 服务器区域的交换机上。
- Internet 接入路由器之后的第一台交换机上。
- 重点保护网段的局域网交换机上。

入侵检测系统往往与防火墙联合部署，常用的部署方法有以下几种。

- 入侵检测探测器放在防火墙之外。
- 入侵检测探测器放在防火墙之内。
- 防火墙内外都有入侵检测探测器。
- 入侵检测探测器安装在其他关键部位。

7.2.8　病毒防护

7.2.8.1　病毒定义

按《中华人民共和国计算机信息系统安全保护条例》中的规定，计算机病毒是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。

在病毒的生存期内，典型的病毒经历了以下 4 个阶段。

(1) 潜伏阶段。

(2) 繁殖阶段。

(3) 触发阶段。

(4) 执行阶段。

7.2.8.2 病毒分类

对于最重要的病毒类型，建议如下的分类方法。

(1) 寄生病毒。寄生病毒将自己附加到可执行文件中，当被感染的程序执行时，找到其他可执行文件并感染。

(2) 存储器驻留病毒。存储器驻留病毒寄宿在主存中，作为驻留程序的一部分。从那时起，病毒感染每个执行的程序。

(3) 引导区病毒。引导区病毒感染主引导记录或引导记录，并且当系统从包含了病毒的磁盘启动时进行传播。

(4) 隐形病毒。隐形病毒能在反病毒软件检测时隐藏自己。

(5) 多形病毒。多形病毒是每次感染都会改变的病毒，使得反病毒软件无法通过病毒的“签名”来检测自己。

7.2.8.3 防病毒技术

在所有计算机安全威胁中，计算机病毒是最为严重的，它不仅发生的频率高、损失大，而且潜伏性强、覆盖面广。计算机病毒具有不可估量的威胁性和破坏力，对它的防范是网络安全技术中重要的一环。防病毒技术包括预防病毒、检测病毒、消除病毒等技术。

7.3 真题详解

7.3.1 综合知识试题

试题 1 (2017 年下半年试题 42)

下列攻击行为中属于典型被动攻击的是__(42)__。

(42)A. 拒绝服务攻击　　B. 会话拦截　　C. 系统干涉　　D. 修改数据命令

参考答案：(42)B。

要点解析：被动攻击是对信息的保密性进行攻击，并不修改信息的内容，其目标是获得正在传送的信息。修改数据命令属于主动攻击。

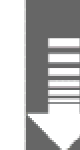
试题 2 (2017 年下半年试题 45)

以下关于入侵检测系统的描述中，正确的是__(45)__。

(45) A. 实现内外网隔离与访问控制
B. 对进出网络的信息进行实时的监测与比对，及时发现攻击行为
C. 隐藏内部网络拓扑
D. 预防、检测和消除网络病毒

参考答案：(45)B。

要点解析：入侵检测系统可以检测出正在发生的攻击活动，发现攻击活动的范围和后果，诊断并发现攻击者的入侵方式和地点，给出解决建议，收集记录入侵活动的证据。



试题 3　(2017 年下半年试题 65)

__(65)__ 不属于入侵检测技术。

(65)A. 专家系统　　B. 模型检测　　C. 简单匹配　　D. 漏洞扫描

参考答案：(65)D。

要点解析：入侵检测技术是指阻止入侵者试图控制自己的系统或者网络资源的安全保护机制，而漏洞扫描是指基于漏洞数据库，通过扫描手段对指定的远程或者本地计算机系统的安全脆弱性进行检测，不属于入侵检测技术。

试题 4　(2017 年上半年试题 37 和试题 38)

PGP 是一种用于电子邮件加密的工具，可提供数据加密和数字签名服务，使用 __(37)__ 进行数据加密，使用 __(38)__ 进行数据完整性验证。

(37)A. RSA　　B. IDEA　　C. MD5　　D. SHA-1

(38)A. RSA　　B. IDEA　　C. MD5　　D. SHA-1

参考答案：(37)B；(38)C。

要点解析：IDEA 叫对称加密算法，其机理是用一个 128bit 的密钥加密明文。在 PGP 中，IDEA 算法被用来加密邮件正文。而非对称加密算法 RSA 主要实现数字签名功能。

进行数据完整性验证则需要使用 MD5 算法。

试题 5　(2017 年上半年试题 39)

IPSec 用于增强 IP 网络的安全性，下面的说法中不正确的是 __(39)__ 。

(39) A. IPSec 可对数据进行完整性保护

B. IPSec 提供用户身份认证服务

C. IPSec 的认证头添加在 TCP 封装内部

D. IPSec 对数据加密传输

参考答案：(39)C。

要点解析：在传输模式下，IPSec 包头添加在原 IP 包头和数据之间，在整个传输层报文段的后面和签名添加一些控制字段，构成 IPSec 数据报。隧道模式是对整个 IP 数据包提供安全传输机制，是在一个 IP 数据包的前面和后面都添加一些控制字段，从而形成 IPSec 数据报。

试题 6　(2017 年上半年试题 41 和试题 42)

三重 DES 加密使用 __(41)__ 个密钥对明文进行 3 次加密，其密钥长度为 __(42)__ 位。

(41)A. 1　　B. 2　　C. 3　　D. 4

(42)A. 56　　B. 112　　C. 128　　D. 168

参考答案：(41)B；(42)B。

要点解析：三重 DES 是指使用两个密钥，执行三次 DES 算法。其密钥长度是 112 位。

试题 7　(2017 年上半年试题 43)

以下加密算法中，适合对大量的明文消息进行加密传输的是 __(43)__ 。

(43)A. RSA　　B. SHA-1　　C. MD5　　D. RC5

参考答案：(43)D。

要点解析：对称密钥密码体制的优点在于效率高，算法简单，系统开销小，适合加密大量数据。答案中仅有 RC5 为对称密码体制。

试题 8 (2017 年上半年试题 44)

假定用户 A、B 分别在 I1 和 I2 两个 CA 处取得了各自的证书，下面 (44) 是 A、B 互信的必要条件。

(44) A. A、B 互换私钥　　B. A、B 互换公钥
C. I1、I2 互换私钥　　D. I1、I2 互换公钥

参考答案：(44)D。

要点解析：两个用户分别取得证书之后，两个 CA 相互交换 CA 的公钥来验证对方身份。

试题 9 (2017 年上半年试题 45)

SHA-1 是一种将不同长度的输入信息转换成 (45) 位固定长度摘要的算法。

(45) A. 128　　B. 160　　C. 256　　D. 512

参考答案：(45)B。

要点解析：SHA 输出 160 比特的摘录。

试题 10 (2016 年下半年试题 43)

下面不属于数字签名作用的是 (43) 。

(43) A. 接收者可验证消息来源的真实性　　B. 发送者无法否认发送过该消息
C. 接收者无法伪造篡改信息　　D. 可验证接收者的合法性

参考答案：(43)D。

要点解析：数字签名应该满足：①接收者能够核实发送者；②发送者事后不能抵赖对报文的签名；③接收者不能伪造对报文的签名。

试题 11 (2016 年下半年试题 44)

下面可用于消息认证的算法是 (44) 。

(44) A. DES　　B. PGP　　C. MD5　　D. KMI

参考答案：(44)C。

要点解析：报文摘要算法 MD5 已获得了广泛的应用，它可对任意长度的报文进行运算，得出 128 位的 MD5 报文摘要代码。除此之外，还有一种和 MD5 相似的安全散列算法 SHA，码长为 160 位，比 MD5 更安全但计算效率不及 MD5。

试题 12 (2016 年下半年试题 45)

DES 加密算法的密钥长度为 56 位，三重 DES 的密钥长度为 (45) 。

(45) A. 168　　B. 128　　C. 112　　D. 56

参考答案：(45)C。

要点解析：三重 DES 是指使用两个密钥，执行三次 DES 算法，其密钥长度是 112 位。

试题 13 (2016 年上半年试题 41、42 和试题 43)

用户 B 收到经 A 数字签名后的消息 M，为验证消息的真实性，首先需要从 CA 获取用



户 A 的数字证书，该数字证书中包含 __(41)__ ，可以利用 __(42)__ 验证该证书的真伪，然后利用 __(43)__ 验证 M 的真实性。

(41) A. A 的公钥　　B. A 的私钥　　C. B 的公钥　　D. B 的私钥
(42) A. CA 的公钥　　B. B 的私钥　　C. A 的公钥　　D. B 的公钥
(43) A. CA 的公钥　　B. B 的私钥　　C. A 的公钥　　D. B 的公钥

参考答案：(41)A；(42)A；(43)C。

要点解析：数字证书颁发的过程为：用户首先产生自己的密钥对，并将公共密钥及部分个人身份信息传送给认证中心。认证中心在核实身份后，将执行一些必要的步骤，以确信请求确实从用户而来，然后认证中心将发给用户一个数字证书，该证书内包含用户的个人信息和他的公钥，同时还附有认证中心的签名信息，用户可以利用认证中心 CA 的公钥验证该证书的真伪。而数字签名是发送方用自己的私钥对信息进行签名，接收方用发送方的公钥对信息进行核实签名。

试题 14　(2016 年上半年试题 44)

3DES 的密钥长度为 __(44)__ 。

(44) A. 56　　B. 112　　C. 128　　D. 168

参考答案：(44)B。

要点解析：DES 使用 56 位密钥加密。3DES 是 DES 加密算法的一种模式，它使用 3 条 56 位的密钥对数据进行三次加密。本质上就相当于用一个长为 168 位的密钥进行加密。若数据对安全性要求不那么高，K1 可以等于 K3，即第一次和第三次采用相同的密钥，在这种情况下，密钥的有效长度为 112 位。

试题 15　(2016 年上半年试题 45)

下列不属于报文认证算法的是 __(45)__ 。

(45) A. MD5　　B. SHA-1　　C. RC4　　D. HMAC

参考答案：(45)C。

要点解析：RC4 加密算法是 1987 年设计的密钥长度可变的流加密算法簇，是一种对称加密算法。该算法的速度可以达到 DES 加密的 10 倍左右，且具有很高级别的非线性，是应用最广泛的流加密算法，应用在安全套接字层(SSL)(用来保护网络上传输的数据)和 WEP(无线网络数据保护)上。

RFC 1321 提出的报文摘要算法 MD5 已获得广泛的应用，它可对任意长度的报文进行运算，得出 128 位的 MD5 报文摘要代码。还有一种安全散列算法 SHA，与 MD5 相似但码长为 160 位，SHA 比 MD5 更安全，但效率较低。另外还有 HAMC(散列消息鉴别码)，是基于密钥的 Hash 算法的认证协议。其原理为：用公开函数和密钥产生一个固定长度的值作为认证标识，用此标识来验证消息的完整性，使用一个密钥生成一个固定大小的小数据块，即 MAC，并将其加入消息中，然后传输。接收方利用与发送方共享的密钥进行鉴别认证。

试题 16　(2015 年下半年试题 41)

__(41)__ 不属于主动攻击。

(41) A. 流量分析　　B. 重放　　C. IP 地址欺骗　　D. 拒绝服务

参考答案：(41)A。

要点解析：计算机网络上的通信面临以下四种威胁。

① 截获：攻击者从网络上窃听他人的通信内容。

② 中断：攻击者有意中断他人在网络上的通信。

③ 篡改：攻击者故意篡改网络中传送的报文。

④ 伪造：攻击者伪造信息在网络上的传送。

以上的四种威胁可以划分为两大类，即被动攻击和主动攻击。在上述情况中，截获信息的攻击属于被动攻击，而中断、篡改和伪造信息的攻击称为主动攻击。

试题 17 (2015 年下半年试题 42 和试题 43)

下列算法中，可用于报文认证的是 (42) ，可以提供数字签名的是 (43) 。

(42) A. RSA　　B. IDEA　　C. RC4　　D. MD5

(43) A. RSA　　B. IDEA　　C. RC4　　D. MD5

参考答案：(42)D；(43)A。

要点解析：报文认证是为了确保数据的完整性和真实性，对报文的来源、时间及目的地进行验证。报文的认证方式有传统加密方式的认证、使用密钥的报文认证码方式、使用单向散列函数的认证和数字签名认证方式。常用于报文认证的算法有 MD5 和 SHA。MD5(Message Digest Algorithm 5)是一种单向散列算法，可以把不同长度的数据块进行暗码运算，产生一个 128 位的数值；SHA(Secure Hash Algorithm)是一种较新的散列算法，可以对任意长度的数据运算生成一个 160 位的数值。

数字签名是一种类似写在纸上的普通的物理签名，但是使用了公钥加密领域的技术实现，用于鉴别数字信息的方法。一套数字签名通常定义两种互补的运算，一个用于签名，另一个用于验证。普通数字签名算法有 RSA、ElGamal、Fiat-Shamir、Guillou-Quisquarter、Schnorr、Ong-Schnorr-Shamir、DES/DSA、椭圆曲线数字签名算法和有限自动机数字签名算法等。

试题 18 (2015 年下半年试题 44)

下列 (44) 不能提供应用层安全。

(44) A. S-HTTP　　B. PGP　　C. MIME　　D. SET

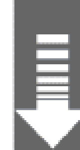
参考答案：(44)C。

要点解析：安全超文本传输协议 S-HTTP 使用在应用层，它是 HTTP 协议的扩展，它仅适用于 HTTP 连接上。S-HTTP 可提供通信保密、身份识别、可信赖的信息传输服务及数字签名等。

PGP 是 1995 年开发出的一个完整的电子邮件安全软件包，包括加密、鉴别、电子签名和压缩等技术。PGP 工作原理并不复杂。其提供电子邮件的安全性、发送鉴别和报文完整性功能。

MIME 意为多目 Internet 邮件扩展，它设计的最初目的是在发送电子邮件时附加多媒体数据，让邮件客户程序能根据其类型进行处理。

SET 协议是专为在因特网上进行安全信用卡交易的协议，最初是由两个著名的信用卡公司 VISA 和 MasterCard 开发的。但是在 SET 交易中客户端要使用专门的软件(浏览器钱包)，



同时商家要支付的费用比使用 SSL 更加昂贵，所以 SET 在市场竞争中失败了。

试题 19 (2015 年下半年试题 45)

防火墙不具备__(45)__功能。

(45) A. 包过滤　　B. 查毒　　C. 记录访问过程　　D. 代理

参考答案：(45)B。

要点解析：具体来说，防火墙主要有以下几方面功能。

① 创建一个检查点。防火墙在一个公司内部网络和外部网络间建立一个检查点。这种实现要求所有的流量都要通过这个检查点。一旦这些检查点清楚地建立，防火墙设备就可以监视、过滤和检查所有进来和出去的流量。

② 隔离不同网络，防止内部信息的外泄。这是防火墙的最基本功能，它通过隔离内、外部网络来确保内部网络的安全，也限制了局部重点或敏感网络安全问题对全局网络造成的影响。

③ 强化网络安全策略。通过以防火墙为中心的安全方案配置，能将所有安全软件(如口令、加密、身份认证、审计等)配置在防火墙上。与将网络安全问题分散到各个主机上相比，防火墙的集中安全管理更方便，更能有效地对网络安全性能起到加强作用。

④ 有效地审计和记录内、外部网络上的活动。防火墙可以对内、外部网络存取和访问进行监控审计。如果所有的访问都经过防火墙，那么，防火墙就能记录下这些访问并进行日志记录，同时也能提供网络使用情况的统计数据。

试题 20 (2015 年下半年试题 47)

为防止 WWW 服务器与浏览器之间传输的信息被窃听，可以采取__(47)__来防止该事件的发生。

(47) A. 禁止浏览器运行 ActiveX 控件
B. 索取 WWW 服务器的 CA 证书
C. 将 WWW 服务器地址放入浏览器的可信站点区域
D. 使用 SSL 对传输的信息进行加密

参考答案：(47)D。

要点解析：SSL 可以对万维网客户与服务器之间传送的数据进行加密和鉴别。在双方握手阶段，对将要使用的加密算法和双方共享的会话密钥进行协商，完成客户与服务器之间的鉴别。在握手完成后，所传送的数据都使用会话密钥进行传输。

试题 21 (2015 年上半年试题 39)

提供电子邮件安全服务的协议是__(39)__。

(39) A. PGP　　B. SET　　C. S-HTTP　　D. Kerberos

参考答案：(39)A。

要点解析：PGP(Pretty Good Privacy)，是一个基于 RSA 公钥加密体系的邮件加密协议。可以用它对邮件保密以防止非授权者阅读，它还能对邮件加上数字签名，从而使收信人可以确认邮件的发送者，并能确信邮件没有被篡改。

试题 22 (2015 年上半年试题 40)

IDS 设备的主要作用是__(40)__。

(40) A. 用户认证　　B. 报文认证
C. 入侵检测　　D. 数据加密

参考答案：(40)C。

要点解析：IDS是入侵检测系统的英文缩写，全称为Intrusion Detection System，顾名思义，IDS设备的主要作用是对网络中的入侵行为进行检测。

试题23 (2015年上半年试题41)

宏病毒可以感染后缀为__(41)__的文件。

(41) A. exe　　B. txt　　C. pdf　　D. xls

参考答案：(41)D。

要点解析：宏病毒的共同特点是能感染Office文档，然后通过Office通用模板进行传播。xls是Excel文档的后缀名，Excel是Office的组件之一，可以被宏病毒感染。

试题24 (2015年上半年试题42)

Kerberos是一种__(42)__。

(42) A. 加密算法　　B. 签名算法　　C. 认证服务　　D. 病毒

参考答案：(42)C。

要点解析：Kerberos是一种网络认证协议，其设计目标是通过密钥系统为客户机/服务器应用程序提供强大的认证服务。该认证过程的实现不依赖于主机操作系统的认证，无须基于主机地址的信任，不要求网络上所有主机的物理安全，并假定网络上传送的数据包可以被任意地读取、修改和插入数据。在以上情况下，Kerberos作为一种可信任的第三方认证服务，是通过传统的密码技术(如共享密钥)执行认证服务的。

试题25 (2015年上半年试题43)

以下关于三重DES加密的叙述中，正确的是__(43)__。

(43) A. 三重DES加密使用一个密钥进行三次加密
B. 三重DES加密使用两个密钥进行三次加密
C. 三重DES加密使用三个密钥进行三次加密
D. 三重DES加密的密钥长度是DES密钥长度的3倍

参考答案：(43)B。

要点解析：三重DES加密使用两个密钥对报文做三次DES加密，效果相当于将DES密钥的长度加倍，DES密钥为56位，则三重DES的密钥长度为112位。

试题26 (2015年上半年试题64)

__(64)__针对TCP连接进行攻击。

(64) A. 拒绝服务　　B. 暴力攻击
C. 网络侦察　　D. 特洛伊木马

参考答案：(64)A。

要点解析：拒绝服务攻击即攻击者想办法让目标机器停止提供服务，是黑客常用的攻击手段之一。SYN Flood是当前最流行的DoS(拒绝服务攻击)与DDoS(Distributed Denial of Service，分布式拒绝服务攻击)的方式之一，这是一种利用TCP协议缺陷，发送大量伪造的



TCP 连接请求，使被攻击方资源耗尽(CPU 满负荷或内存不足)的攻击方式。

7.3.2　案例分析试题

试题 1　(2017 年下半年下午试题一)

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】某企业组网方案如图 7.31 所示，网络接口规划如表 7.3 所示。公司内部员工和外部访客均可通过无线网络访问企业网络，内部员工无线网络的 SSID 为 Employee，访客无线网络的 SSID 为 Visitor。

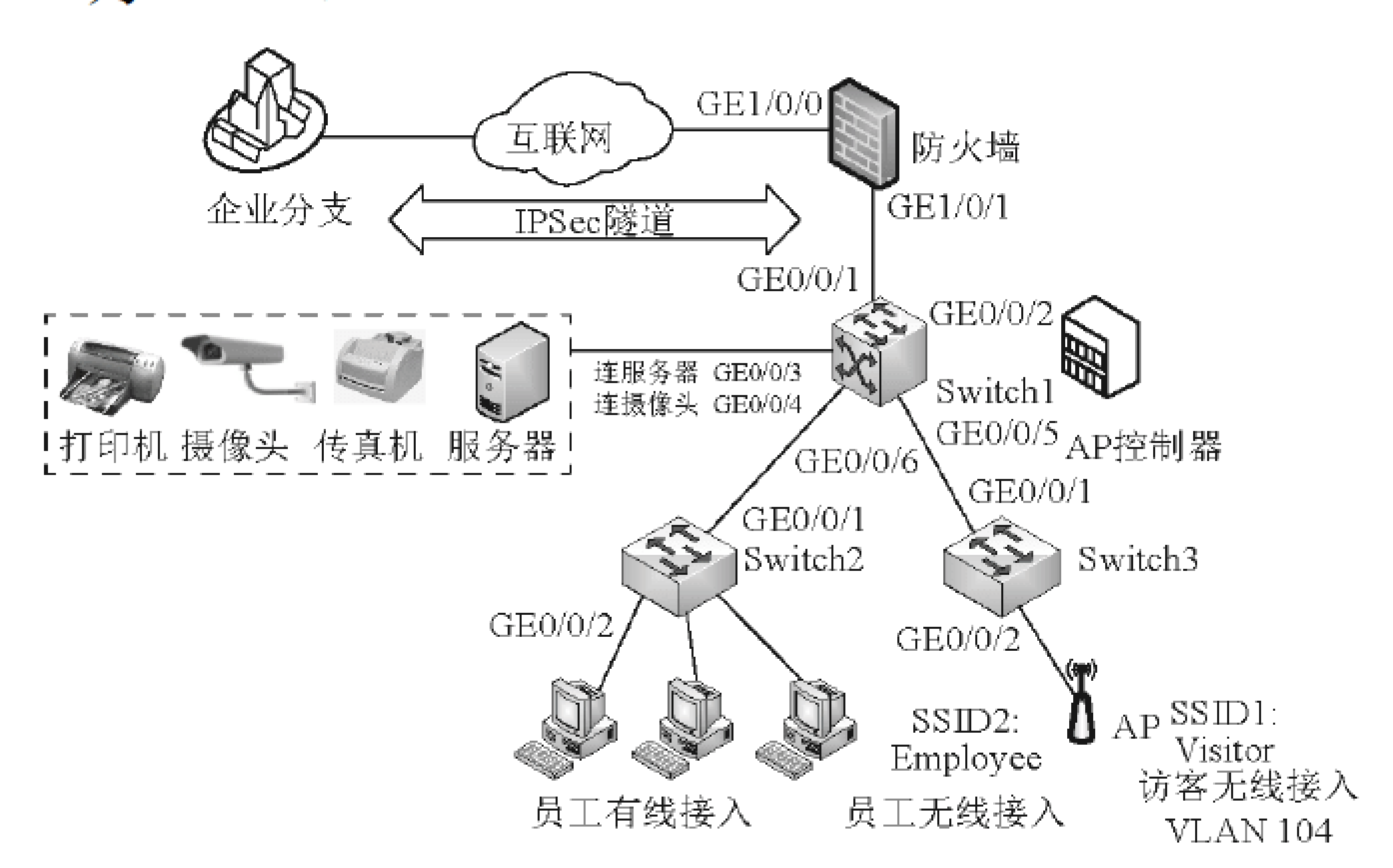


图 7.31　某企业组网方案

表 7.3　网络接口规划

设 备 名	接口编号	所属 VLAN	IP 地址
防火墙	GE1/0/0	—	200.1.1.1/24
	GE1/0/1	—	192.168.99.254/24
AP 控制器	GE0/0/1	10	VLANIF10：192.168.10.1/24
Switch1	GE0/0/1	99	VLANIF10：192.168.10.254/24 VLANIF99：192.168.99.1/24 VLANIF100：192.168.100.1/24 VLANIF101：192.168.101.1/24 VLANIF102：192.168.102.1/24 VLANIF103：192.168.103.1/24 VLANIF104：192.168.104.1/24
	GE0/0/2	10	
	GE0/0/3	101	
	GE0/0/4	102	
	GE0/0/5	100、103、104	
	GE0/0/6	100	
Switch2	GE0/0/1	100	—
	GE0/0/2	100	—
Switch3	GE0/0/1	100、103、104	—
	GE0/0/2	100、103、104	—

【问题 1】(6 分)

防火墙上配置 NAT 功能，用于公私网地址转换。同时配置安全策略，将内网终端用户所在区域划分为 Trust 区域，外网划分为 Untrust 区域，保护企业内网免受外部网络攻击。

补充防火墙数据规划表7.4内容中的空缺项。

表 7.4　防火墙数据规划

安全策略	源安全域	目的安全域	源地址/区域	目的地址/区域
egress	Trust	Untrust	192.168.100.0/24 192.168.101.0/24 192.168.103.0/24 192.168.104.0/24	—
local_untrust	Local	Untrust	(1)	200.1.1.2/32
untrust_local	Untrust	Local	Untrust	(2)
NAT 策略(转换前)	Trust	Untrust	Srcip	(3)

注：Local 表示防火墙本地区域；Srcip 表示源 IP。

【问题 2】(4 分)

在点到点的环境下，配置 IPSec VPN 隧道需要明确＿(4)＿和＿(5)＿。

【问题 3】(6 分)

在 Switch1 上配置 ACL 禁止访客访问内部网络，将 Switch1 数据规划表 7.5 内容中的空缺项补充完整。

表 7.5　Switch1 数据规划

项　目	VLAN	源 IP	目的 IP	动　作
ACL	(6)	(7)	192.168.100.0/0.0.0.255 192.168.101.0/0.0.0.255 192.168.102.0/0.0.0.255 192.168.103.0/0.0.0.255	(8)

【问题 4】(4 分)

AP 控制器上部署 WLAN 业务，采用直接转发，AP 跨三层上线。认证方式：无线用户通过预共享密钥方式接入。

在 Switch1 上 GE0/0/2 端口连接 AP 控制器，该接口类型配置为＿(9)＿模式，所在 VLAN 是＿(10)＿。

参考答案：

【问题 1】(1)192.168.99.0124；(2)200.1.1.1/32；(3)Any。

【问题 2】(4)IP 地址；(5)隧道名称、双方的密钥。

【问题 3】(6)VLAN 104；(7)192.168.104.010.0.0.255；(8)Deny。

【问题 4】(9)Access；(10)VLAN 10。

要点解析：

【问题 1】Local 表示防火墙本地区域，即直连网段。

【问题 2】企业网通过 IPSec 隧道与分支相连，因此需要配置隧道的源 IP 地址和目的 IP 地址以及隧道名称、双方的密钥。



【问题 3】要通过 ACL 实现访问控制：禁止访客访问内部网络。访客对应网段为 VLAN 104 即 192.168.104.0/24，动作应为 Deny。

【问题 4】AP 控制器连接在核心交换机的 GE0/0/2 端口，对应 VLAN 为 100，因此端口类型为 Access。

试题 2 （2017 年上半年下午试题二）

阅读下列说明，回答问题 1 至问题 3，将解答填入答题纸的对应栏内。

【说明】某公司的网络拓扑结构图如图 7.32 所示。

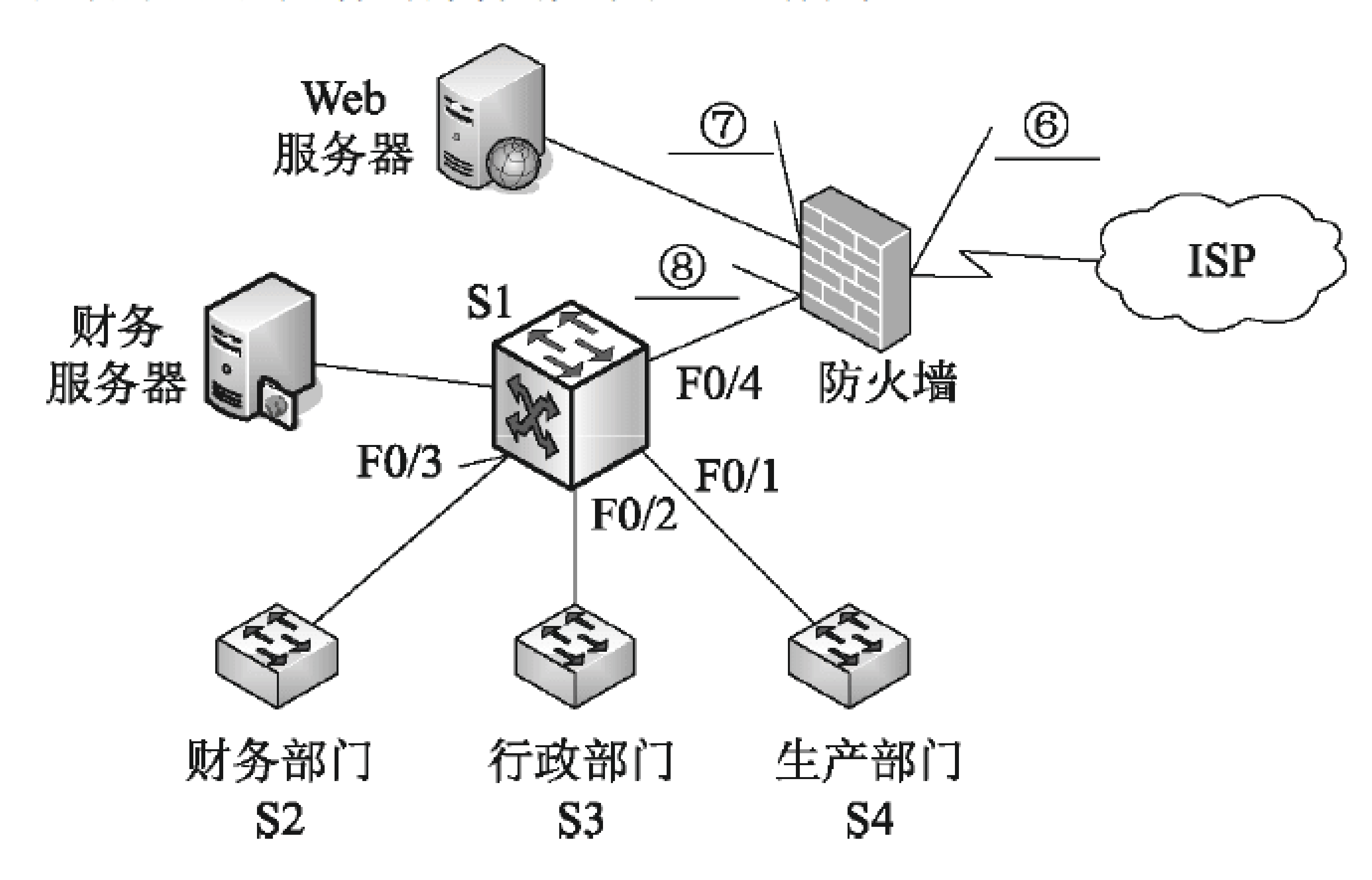


图 7.32　网络拓扑结构图

【问题 1】(共 5 分)

为了保障网络安全，该公司安装了一款防火墙，对内部网络、服务器以及外部网络进行逻辑隔离，其网络结构如图 7.32 所示。

包过滤防火墙使用 ACL 实现过滤功能，常用的 ACL 分为两种，编号为<u>　(1)　</u>的 ACL 根据 IP 报文的<u>　(2)　</u>域进行过滤，称为<u>　(3)　</u>；编号为<u>　(4)　</u>的 ACL 根据 IP 报文中的更多域对数据包进行控制，称为<u>　(5)　</u>。

(1)～(5)备选项：

A. 标准访问控制列表

B. 扩展访问控制列表

C. 基于时间的访问控制列表

D. 1～99

E. 0～99

F. 100～199

G. 目的 IP 地址

H. 源 IP 地址

I. 源端口

J. 目的端口

【问题 2】(共 6 分)

如图 7.32 所示，防火墙的三个端口，端口⑥是<u>　(6)　</u>、端口⑦是<u>　(7)　</u>、端口⑧是<u>　(8)　</u>。

(6)～(8)备选项：

A. 外部网络　　B. 内部网络　　C. 非军事区

【问题 3】(共 9 分)

公司内部 IP 地址分配如表 7.6 所示。

表 7.6　公司内部 IP 地址分配

部门/服务器	IP 地址段
财务部门	192.168.9.0/24
生产部门	192.168.10.0/24
行政部门	192.168.11.0/24
财务服务器	192.168.100.1/24
Web 服务器	10.10.200.1/24

1. 为保护内网安全，防火墙的安全配置要求如下。

(1) 内外网用户均可访问 Web 服务器，特定主机 200.120.100.1 可以通过 Telnet 访问 Web 服务器。

(2) 禁止外网用户访问财务服务器，禁止财务部门访问 Internet，允许生产部门和行政部门访问 Internet。

根据以上需求，请按照防火墙的最小特权原则补充完成表 7.7。

表 7.7　配置信息表

序　号	源地址	源端口	目的地址	目的端口	协　议	规　则
1	Any	Any	(9)	(10)	WWW	允许
2	(11)	Any	10.10.200.1	(12)	Telnet	允许
3	(13)	Any	Any	Any	Any	(14)
4	Any	Any	Any	Any	Any	(15)

2. 若调换上面配置中的第 3 条和第 4 条规则的顺序，则 (16) 。

(16) 备选项：

A. 安全规则不发生变化　　B. 财务服务器将受到安全威胁

C. Web 服务器将受到安全威胁　　D. 内网用户将无法访问 Internet

3. 在上面的配置中，是否实现了“禁止外网用户访问财务服务器”这条规则?

参考答案：

【问题 1】(1)D；(2)H；(3)A；(4)F；(5)B。

【问题 2】(6)A；(7)C；(8)B。

【问题 3】1. (9)10.10.200.1；(10)80；(11)200.120.100.1；(12)23；(13)192.168.10.0；(14)允许；(15)拒绝。

2. (16)D。

3. 已经实现，除了允许的，其余均已经禁止。

要点解析：

【问题 1】访问控制列表用来限制使用者或设备，以达到控制网络流量，解决网络拥塞，提高安全性的目的。IP 访问控制列表主要有两种类型：标准访问控制列表和扩展访问控制

列表。标准访问控制列表只对数据包中的源地址进行检查，以此来判定是否允许数据包通过，其表号为 1～99。扩展访问控制列表除了检查源地址和目的地址外，还可以检查指定的协议或端口号，来对数据包进行过滤，其表号为 100～199。

【问题 2】防火墙通常至少具有 3 个接口，当使用具有 3 个接口的防火墙时，会产生至少 3 个网络。内部网络(内网)通常是指企业内部网络或者企业内部网络的一部分。它是互联网的信任区域，即受到了防火墙的保护。外部网络(外网)通常指 Internet 或者非企业内部网络。它是互联网中不被信任的区域，当外部区域想要访问内部区域的主机和服务器时，通过设置防火墙就可以实现有限制的访问。非军事区(DMZ，又称停火区)是一个隔离的网络或几个网络。位于非军事区中的主机或服务器被称为堡垒主机。一般在非军事区内可以放置 Web 服务器和 Mail 服务器等。非军事区对于外部用户通常是可以访问的，这种方式允许外部用户访问企业的公开信息，但不允许他们访问企业内部网络。

【问题 3】访问控制列表就是用来在路由技术的网络中，决定这些数据流量是应该被转发还是被丢弃的技术。因此访问控制列表就成了实现防火墙的重要手段。设置 ACL 的规则主要是：按顺序依行进行比较，从第一行起直到找到一个符合条件的行，符合之后，其余的行就无须比较了。默认在 ACL 中最后一行都隐藏拒绝所有，如果之前没找到一条 permit 语句，则意味着该包将被丢弃。所以每个 ACL 中都应该至少有一行 permit 语句，除非用户想把所有的数据包丢弃。

如果 3 和 4 两行的顺序调换会导致内网的用户无法访问互联网。

禁止外网访问财务服务器已经实现，因为配置中除了被允许的，其余均已禁止。

试题 3 (2016 年下半年下午试题一)

阅读以下说明，回答问题 1 至问题 6，将解答填入答题纸对应的解答栏内。

【说明】某企业的行政部、技术部和生产部分布在三个区域，随着企业对信息化需求的提高，现拟将网络出口链路由单链路升级为双链路，提升 ERP 系统服务能力以及加强员工上网行为管控。网络管理员依据企业现有网络和新的网络需求设计了该企业网络拓扑图 7.33，并对网络地址重新进行了规划，其中防火墙设备继承了传统防火墙与路由功能。

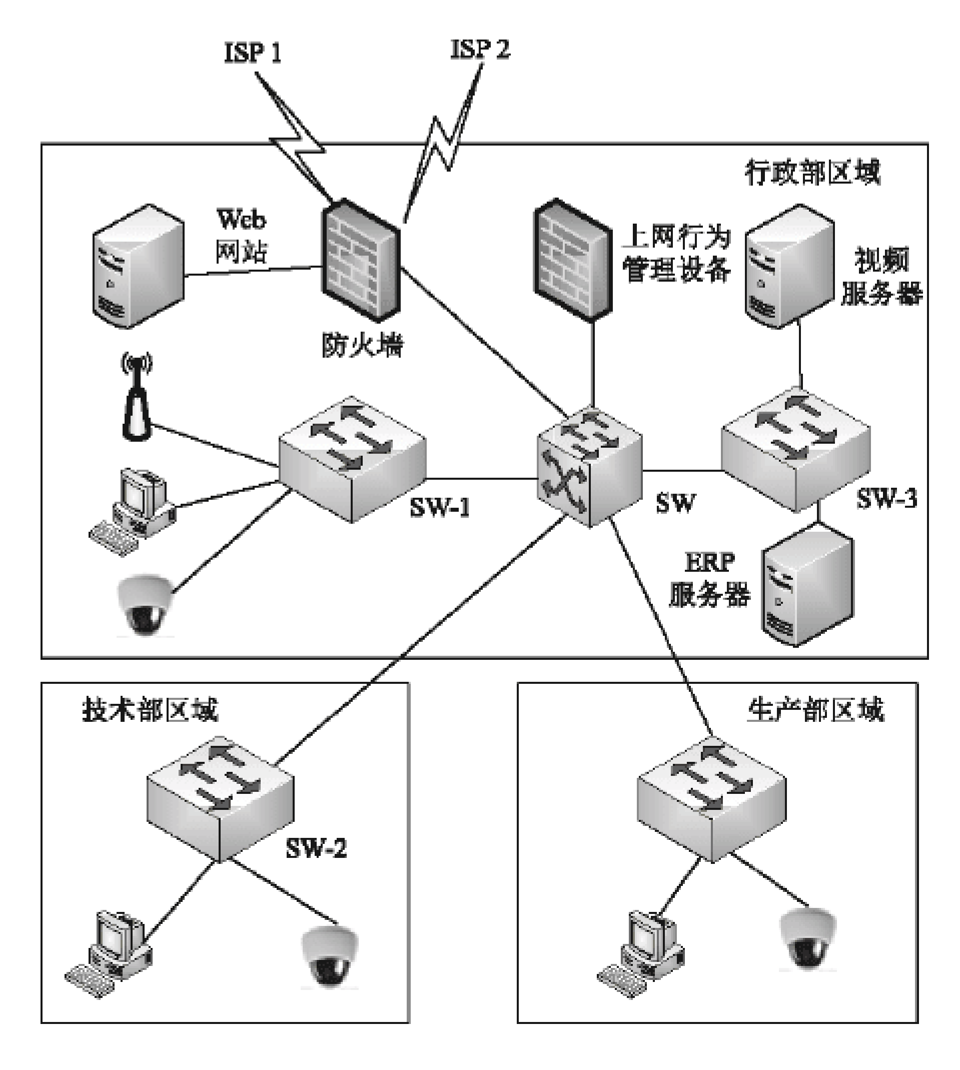


图 7.33　网络拓扑图

【问题 1】 (4 分)

在图 7.33 的防火墙设备中，配置双出口链路有提高总带宽、__(1)__、链路负载均衡作用。通过配置链路聚合来提高总带宽，通过配置__(2)__来实现链路负载均衡。

【问题 2】 (4 分)

防火墙工作模式有路由模式、透明模式、混合模式，若该防火墙接口均配有 IP 地址，则防火墙工作在__(3)__模式。该模式下，ERP 服务器部署在防火墙的__(4)__区域。

【问题 3】 (4 分)

若地址规划如表 7.8 所示，从 IP 规划方案看该地址的配置可能有哪些方面的考虑？

表 7.8　地址规划表

位置或系统	VLAN ID	地址区间	信息点数量	备　注
行政部	10～13	192.168.10.0～192.168.13.0	60	网段按楼层分配，每个网段末位地址为网关
技术部	14～17	192.168.14.0～192.168.17.0	80	
生产部	18～20	192.168.18.0～192.168.20.0	30	
无线网络	22	192.168.22.0		行政楼区域部署
监控网络	23	192.168.23.0	30	信息点分散
ERP	30	192.168.30.0		

【问题 4】 (3 分)

该网络拓扑中，上网行为管理设备的位置是否合适？请说明理由。

【问题 5】 (3 分)

该网络中有无线节点的接入，在安全管理方面应采取哪些措施？

【问题 6】(2 分)

该网络中视频监控系统与数据业务共用网络带宽，存在哪些弊端？

参考答案：

【问题 1】(1)链路备份/冗余；(2)策略路由。

【问题 2】(3)路由；(4)内部/inside。

【问题 3】各部门终端数的扩展考虑，增加部门或部门 VLAN 的考虑，监控以及部门中信息点增加的扩展考虑。

【问题 4】不合适，应该部署在防火墙与核心交换机间，使用跨接/串联的方式接入。因为需要对用户上网行为进行管控，需要保证上网数据流经上网行为管理设备。

【问题 5】接入认证、无线加密、隐藏 SSID、授权管理、审计管理(本题分值为 3 分，答对 3 个即可)。

【问题 6】视频监控系统业务流量大，如果带宽不足会影响数据业务的通信速率。

要点解析：

【问题 1】双出口链路的作用有：

① 可以实现带宽增加：当原先的单出口带宽不足时，可通过双出口增加出口带宽。

② 链路冗余：一条链路故障也保证网络联通，起到冗余备份的作用。

③ 负载均衡：负载均衡是将双出口的流量合理地分担到外网，可以通过专用负载均



衡设备(增加成本)，也可以使用路由器的策略路由实现基于源或目的以及业务类型等的负载分担，同时也可以直接配置等价默认路由+NAT 双 outside 接口做等价负载均衡。

【问题 2】防火墙三种工作模式的区别。

① 路由模式：内部网络和外部网络属于不同的子网，需要重新规划原有的网络拓扑，接口需要配置 IP 地址，接口所在的安全区域是三层区域。

② 透明模式：内部网络和外部网络属于相同的子网，无须改变原有的网络拓扑，接口不能配置 IP 地址，接口所在的安全区域是二层区域。

③ 混合模式：混合模式介于路由模式和透明模式，既可以配置接口工作在路由模式(接口具有 IP 地址)，又可以配置接口工作在透明模式(接口无 IP 地址)，主要在 Eudemon 1000G 进行双机热备时使用。

由于防火墙接口均配有 IP 地址，很明显工作于路由模式；在拓扑图上可以直接观察到 Web 服务器部署在 DMZ(非军事)区域，ERP 服务器部署在内网区域。

【问题 3】从 IP 规划方案来看，每个部门划分三个 VLAN，分配的 IP 子网为 192.168.10.0～192.168.20.0，其他未被使用的 192.168.X.0 子网可供扩展的 VLAN 或部门使用，每个 VLAN 规划的子网可用主机数大于目前的信息点数，从以后的网络扩展角度来看，VLAN 中或部门的信息点数的增加，包括无线网络和监控网络的信息点的增加，都可以直接使用未使用的可用主机地址，而不需要重新增加子网或 VLAN。

【问题 4】上网行为管理设备的位置应该保证内网用户的上网流量经过其设备，从而实现行为管理策略。

【问题 5】WLAN 基本安全主要是无线接入和加密，其措施可以有 SSID 隐藏、WEP 或 WPA/WAP2 加密、MAC 地址过滤等。当然对于更负责的安全管理还可以结合 AAA 系统做认证、授权、计费管理甚至审计等。

7.4 强化训练

7.4.1 综合知识试题

试题 1 (2014 年下半年试题 41)

假设有证书发放机构 I1、I2，用户 A 在 I1 获取证书，用户 B 在 I2 获取证书，I1 和 I2 已安全交换了各自的公钥，如果用 I1《A》表示由 I1 颁发给 A 的证书，A 可通过__(41)__证书获取 B 的公开密钥。

(41) A. I1《I2》I2《B》　　B. I2《B》I1《I2》
C. I1《B》I2《I2》　　D. I2《I2》I2《B》

试题 2 (2014 年下半年试题 42、43 和试题 44)

PGP(Pretty Good Privacy)是一种电子邮件加密软件包，它提供数据加密和数字签名两种服务，采用__(42)__进行身份认证，使用__(43)__(128 位密钥)进行数据加密，使用__(44)__进行数据完整性验证。

(42) A. RSA 公钥证书　B. RSA 私钥证书　C. Kerboros 证书　D. DES 私钥证书
(43) A. IDEA　B. RSA　C. DES　D. Diffie-Hellman
(44) A. Hash　B. MD5　C. 三重 DES　D. SHA-1

试题 3　(2014 年下半年试题 45)

以下关于 S-HTTP 的描述中，正确的是__(45)__。

(45) A. S-HTTP 是一种面向报文的安全通信协议，使用 TCP 443 端口
B. S-HTTP 所使用的语法和报文格式与 HTTP 相同
C. S-HTTP 也可以写为 HTTPS
D. S-HTTP 的安全基础并非 SSL

试题 4　(2014 年上半年试题 41)

高级加密标准 AES 支持的 3 种密钥长度不包括__(41)__。

(41) A. 56　B. 128　C. 192　D. 256

试题 5　(2014 年上半年试题 42)

在报文摘要算法 MD5 中，首先要进行明文分组与填充，其中分组时明文报文要按照__(42)__位分组。

(42) A. 128　B. 256　C. 512　D. 1024

试题 6　(2014 年上半年试题 43)

以下关于 IPSec 协议的描述中，正确的是__(43)__。

(43) A. IPSec 认证头(AH)不提供数据加密服务
B. IPSec 封装安全载荷(ESP)用于数据完整性认证和数据源认证
C. IPSec 的传输模式对原来的 IP 数据报进行了封装和加密，再加上了新的 IP 头
D. IPSec 通过应用层的 Web 服务建立安全连接

试题 7　(2014 年上半年试题 44)

防火墙的工作层次是决定防火墙效率及安全的主要因素，下面的叙述中正确的是__(44)__。

(44) A. 防火墙工作层次越低，工作效率越高，安全性越高
B. 防火墙工作层次越低，工作效率越低，安全性越低
C. 防火墙工作层次越高，工作效率越高，安全性越低
D. 防火墙工作层次越高，工作效率越低，安全性越高

试题 8　(2014 年上半年试题 45)

在入侵检测系统中，事件分析器接收事件信息并对其进行分析，判断是否为入侵行为或异常现象，其常用的三种分析方法不包括__(45)__。

(45)A. 模式匹配　B. 密文分析　C. 数据完整性分析　D. 系统分析

7.4.2　综合知识试题参考答案

【试题 1】答　案：(41)A。





解　析：数字证书是一个经证书认证中心(CA)数字签名的包含公开密钥拥有者信息以及公开密钥的文件。由于一个公钥用户拥有的可信任管理中心数量有限，要与大量不同管理域的用户建立安全通信需要 CA 间建立信任关系。一个证书链是从一个自签名的根证书开始，前一个证书主体是后一个证书的发放者。

【试题 2】答　案：(42)A；(43)A；(44)B。

解　析：PGP 是英文 Pretty Good Privacy(更好地保护隐私)的简称，是一个基于 RSA 公钥&私钥及 AES 等加密算法的加密软件系列。PGP 使用 RSA 公钥证书进行身份认证，使用 IDEA(128 位密钥)进行数据加密，使用 MD5 进行数据完整性认证。

【试题 3】答　案：(45)D。

解　析：安全超文本传输协议(Secure Hypertext Transfer Protocol，S-HTTP)是一种结合 HTTP 而设计的消息安全通信协议。S-HTTP 的设计基于与 HTTP 信息样板共存并易于与 HTTP 应用程序相整合。

S-HTTP 为 HTTP 客户机和服务器提供了多种安全机制，这些安全服务选项是适用于万维网上各类用户的，还为客户机和服务器提供了对称能力(及时处理请求和回复，以及两者的参数选择)，同时维持 HTTP 的通信模型和实时特征。

S-HTTP 不需要客户方的公用密钥证明(或公用密钥)，但它支持对称密钥的操作模式。这点很重要，因为这意味着在没有要求用户个人建立公用密钥的情况下，会自发地发生私人交易。它支持端对端安全传输，客户机可能首先启动安全传输(使用报头的信息)，用来支持加密技术。

在语法上，S-HTTP 报文与 HTTP 相同，由请求行或状态行组成，后面是信头和主体。请求报文的格式由请求行、通用信息头、请求头、实体头、信息主体组成。响应报文由响应行、通用信息头、响应头、实体头、信息主体组成。

【试题 4】答　案：(41)A。

解　析：密码学中的高级加密标准(Advanced Encryption Standard，AES)，又称 Rijndael 加密法，是美国联邦政府采用的一种区块加密标准。这个标准用来替代原先的 DES，已经被多方分析且广为全世界所使用。

AES 的基本要求是，采用对称分组密码体制，密钥长度的最少支持为 128、192、256，分组长度 128 位，算法应易于各种硬件和软件实现。

【试题 5】答　案：(42)C。

解　析：Hash 函数又称为杂凑函数、散列函数，它提供了这样的一种计算过程：输入一个长度不固定的字符串，返回一串定长的字符串(又称为 Hash 值)。单向 Hash 函数用于产生信息摘要。

信息摘要简要地描述了一份较长的信息或文件，它可以被看作是一份长文件的数字指纹，信息摘要可以用于创建数字签名，对于特定的文件而言，信息摘要是唯一的，而且不同的文件必将产生不同的信息摘要。常见的信息摘要算法包括 MD5(产生一个 128 位的输出，输入是以 512 位的分组进行处理的)和 SHA(安全散列算法，也是按 512 位的分组进行处理，产生一个 160 位的输出)，它们可以用来保护数据的完整性。

【试题 6】答　案：(43)A。

解　析：Internet 协议安全性(IPSec)是一种开放标准的框架结构，通过使用加密的安全

服务以确保在 Internet 协议(IP)网络上进行保密而安全的通信。

IPSec(Internet Protocol Security)是安全联网的长期方向。它通过端对端的安全性来提供主动的保护以防止专用网络与 Internet 的攻击。在通信中，只有发送方和接收方才是唯一必须了解 IPSec 保护的计算机。

IPSec 协议工作在 OSI 模型的第三层，使其在单独使用时适于保护给予 TCP 或 UDP 的协议(如安全套接层(SSL)就不能保护 UDP 层的通信流)。

与 IPSec 安全相关的协议是 AH 和 ESP。

AH 协议用来向 IP 通信提供数据完整性和身份验证，同时可以提供抗重放服务。

ESP 提供 IP 层加密保证和验证数据源以对付网络上的监听。因为 AH 虽然可以保护通信免受篡改，但并不对数据进行变形转换，数据对于黑客而言仍然是清晰的。

为了有效地保证数据传输安全，在 IPv6 中有另外一个报头 ESP，进一步提供数据保密性并防止篡改。

【试题 7】**答　案**：(44)D。

解　析：防火墙是一种网络安全保障手段，是网络通信时执行的一种访问控制尺度，其主要目的就是控制入、出一个网络的权限，迫使所有的连接都经过这样的检查，防止一个需要保护的网络遭受外界因素的干扰和破坏。在逻辑上，防火墙是一个分离器、一个限制器，也是一个分析器，有效地监视内部网络和 Internet 之间的任何活动，保证内部网络的安全；在物理实现上，防火墙是位于网络特殊位置的一组硬件设备——路由器、计算机或其他特制的硬件设备。防火墙可以是一个独立的系统，也可以在一个进行网络互连的路由器上实现防火墙。

【试题 8】**答　案**：(45)B。

解　析：事件分析器接收事件信息，对其进行分析，判断是否为入侵行为或异常现象，最后将判断的结果转变为告警信息。分析方法有如下三种。

(1) 模式匹配：将收集到的信息与已知的网络入侵和系统误用模式数据库进行比较，从而发现违背安全策略的行为。

(2) 统计分析：首先给系统对象(如用户、文件、目录和设备等)创建一个统计描述，统计正常使用时的一些测量属性(如访问次数、操作失败次数和延时等)；测量属性的平均值和偏差将被用来与网络、系统的行为进行比较，任何观察值在正常值范围之外时，就认为有入侵发生。

(3) 完整性分析(往往用于事后分析)：主要关注某个文件或对象是否被更改。

第 8 章 网络操作系统与应用服务器的配置

8.1 备考指南

8.1.1 考纲要求

根据考试大纲中相应的考核要求，在“网络操作系统与应用服务器的配置”知识模块上，要求考生掌握以下方面的内容。

(1) 网络操作系统的功能、分类和特点。

(2) 网络设备驱动程序(ODI、NDIS)。

(3) Windows Server 2008 R2。

(4) ISA 2004。

(5) Red Hat Enterprise Linux 7。

(6) DHCP 服务器的原理和配置(Windows)。

(7) 网络系统管理，包括 Windows 系统、Windows 活动目录、Windows 终端服务与远程管理。

(8) DNS，包括域名解析、DNS 服务器的配置(Windows)。

(9) 电子邮件服务器配置(Windows)。

(10) WWW，包括虚拟主机、WWW 服务器配置(Windows)、WWW 服务器的安全配置。

(11) 代理服务器的配置(Windows)。

(12) FTP 服务器，包括 FTP 服务器的访问、FTP 服务器的配置(Windows)。

8.1.2 考点统计

“网络操作系统与应用服务器的配置”知识模块在历次网络工程师考试试卷中出现的

考核知识点及分值分布情况如表8.1所示。

表8.1 历年考点统计表

年份	题号	知识点	分值
2017年下半年	上午：31～37、43、61	Linux文件操作命令、Linux基本服务、DNS、DHCP配置	9分
	下午：试题三	Windows Server 2008配置	20分
2017年上半年	上午：31～36、40	Linux文件组织结构、Linux文件操作命令、Windows操作系统	7分
	下午：试题三	Windows服务器的安装与配置	20分
2016年下半年	上午：30～33、39～42、46、49	Windows/Linux网络管理命令、DHCP服务、FTP服务器	10分
	下午：试题三	Windows Server 2003系统的Web、DNS配置	20分
2016年上半年	上午：35～36、50	Linux系统Apache服务、Linux基本知识	3分
	下午：试题三	Windows Server 2003 DHCP、DNS和Web配置服务	20分
2015年下半年	上午：31、32、39、40	Linux文件操作命令、Linux配置文件、电子邮件服务配置	4分
	下午：试题三	Windows Server 2003服务器Web、FTP和邮件服务配置	20分
2015年上半年	上午：27、29～31、33	IIS身份验证方式、Linux网络配置文件、IPSec策略设置、组策略	5分
	下午：试题二、试题三	Linux服务器DHCP服务的配置、Windows Server 2003 FTP和DHCP配置服务	40分
2014年下半年	上午：31、32、35、38、40、49	Linux系统DNS服务器配置	6分
	下午：试题二	远程桌面服务和IIS配置	20分
2014年上半年	上午：31、32、46	Linux网络管理命令、Windows概念	3分
	下午：试题二、试题三	Web服务器配置；Linux系统下构建DNS、DHCP和Web服务器	40分
2013年下半年	上午：31、32	Linux文件操作命令、常用Linux的命令	4分
	下午：试题三	Windows Server 2003系统的Web、DNS和DHCP配置	20分
2013年上半年	上午：32	Grep命令	2分
	下午：试题三	Windows Sever 2003中终端服务的配置、Windows Sever 2003中本地用户安全策略的设置与活动目录	20分
2012年下半年	上午：无		0分
	下午：试题二	Linux中的vsftpd	15分
2012年上半年	上午：无		0分
	下午：试题二、试题三	Linux系统中的DHCP协议配置、Linux中Web服务器、DNS服务器的配置	30分

8.1.3 命题特点

纵观历年试卷，本章知识点是以选择题和综合分析题的形式出现在试卷中的。本章知识点在历次考试上午试卷中，所考查的题量为8～10道选择题，所占分值为8～10分（占试

卷总分值 75 分中的 10%～13%)；在下午试卷中，所考查的题量为 2～3 道综合分析题，所占分值为 30～45 分(占试卷总分值 75 分中的 40%～60%)。大多数试题偏重于实践应用，检验考生是否理解相关的理论知识点和实践经验，考试难度中等偏难。从知识点考查深度的角度分析，每次考试这部分试题在“识记、理解、应用”3 个层面上所占的比例大致为 1∶1∶3。

8.2　考点串讲

8.2.1　Windows Server 2008 R2 的安装与配置

Windows Server 2008 R2 是 Windows Server 2008 的升级产品，为一款仅支持 64 位的操作系统，可以为大、中或小型企业搭建功能强大的网站和应用程序服务器平台。强大的管理功能与经过强化的安全措施，简化了服务器的管理，提高了资源的可用性，有效保护企业应用程序和数据。另外提供了全新的虚拟化技术，提供更多的高级功能，在改善 IT 效率的同时提高了灵活性。无论是整合服务器，构建私有云，或提供虚拟桌面基础架构(VDI)，强大的虚拟化功能，可以将数据中心与桌面的虚拟化战略提升到一个新的层次。

8.2.1.1　Windows Server 2008 R2 的新增功能

Windows Server 2008 R2 增强了核心 Windows Server 操作系统的功能，提供了富有价值的新功能，以协助各种规模的企业提高控制能力、可用性和灵活性，适应不断变化的业务需求。新的 Web 工具、虚拟化技术、可伸缩性增强和管理工具有助于节省时间、降低成本，并为信息技术(IT)基础结构奠定坚实的基础。

Windows Server 2008 R2 包含了许多增强功能，从而使该版本成为有史以来最可靠的 Windows Server Web 应用程序平台。该版本提供了最新的 Web 服务器角色和 Internet 信息服务 IIS7.5 版，并在服务器核心提供了对.NET 更强大的支持。IIS 7.5 的设计目标着重于功能改进，使网络管理员可以更轻松地部署和管理 Web 应用程序，以增强可靠性和可伸缩性。另外，IIS 7.5 简化了管理功能，并为自定义 Web 服务环境提供了比以往更多的方法。

8.2.1.2　Windows Server 2008 R2 的安装

Windows Server 2008 R2 家族包括 Windows Server 2008 R2 基础版、Windows Server 2008 R2 标准版、Windows Server 2008 R2 企业版、Windows Server 2008 R2 数据中心版、Windows Server 2008 R2 Web 版等产品，安装时用户可以进行选择。安装时系统的硬件环境建议 CPU 主频在 1.4 GHz(x64 处理器)以上，内存 512MB 以上，硬盘 32GB 以上，监视器的分辨率在 800 像素×600 像素以上。

Windows Server 2008 R2 的安装继承了 Windows 产品安装时方便、快捷、高效的特点，几乎不需要多少人工参与就可以自动完成硬件的检测、安装、配置等工作。用户需要做的仅是通过屏幕来了解它所提供的各项新技术以及产品特点。安装过程中会收集区域信息、语言信息、个人注册信息、计算机/管理员基本信息、网络基本信息等。

8.2.1.3　Windows Server 2008 R2 的基本配置

1.　本地用户和组

为了保障计算机与网络的安全，Windows Server 2008 R2 为不同的用户设置了不同的权限，同时通过将具有同一权限的用户设置为一个组来简化对用户的管理。

组是从 Windows NT 系统继承下来的安全管理形式，是指多个对象的集合，对象可包括用户、计算机、联系人及其他组。组账户是用户账户的集合，包括了那些具有相同权限的用户账户。当某个用户成员加入一个组时，则该用户也将被赋予该组具有的所有权限。用户也可以同时属于多个组，并且拥有他所加入组的所有权限。组文件夹中的默认组有 Administrator、Backup Operator、Guests、Help Services Group、Network Configuration Operator、Performance Log Users、Performance Monitor Users、Power Users、Print Operators、Remote Desktop Users、Replicator、Telnet Clients、Users。

2.　配置网络协议

只有在计算机上正确安装网卡驱动程序和网络协议，并正确设置 IP 地址信息之后，服务器才能与网络内的计算机进行正常通信。

正确安装网卡驱动和网络协议，并正确配置 IP 地址信息是服务器与计算机进行正常通信的基础。配置网络协议主要是指配置 TCP/IP 协议，包括 IP 地址、子网掩码、默认网关、DNS 和 WINS 等。具体操作为：选择“开始”→“控制面板”→“网络连接”→“本地连接”命令，打开“本地连接 状态”对话框，单击“属性”按钮；打开“本地连接 属性”对话框，选中“Internet 协议(TCP/IP)”选项，单击“属性”按钮；打开“Internet 协议版本 4(TCP/IPv4)属性”对话框，然后进行设置，如图 8.1 所示。

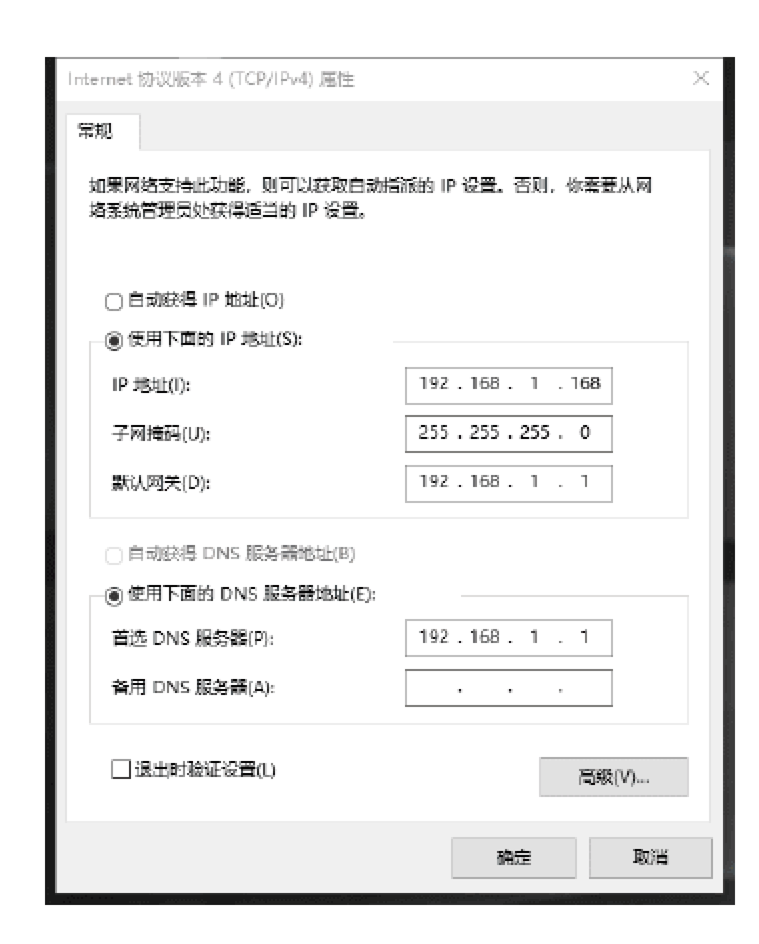


图 8.1　“Internet 协议版本 4 (TCP/IPv4)属性”对话框

3.　添加、删除和管理服务器角色

安装 Windows Server 2008 R2 时，在默认的情况下并不安装任何网络服务，要提供网络服务，必须添加相应的服务器角色，如 DNS 服务器、远程桌面服务、文件服务等。

8.2.1.4　远程管理

1. Windows Server 2008 R2 远程桌面服务

终端服务提供通过作为终端仿真器工作的“瘦客户”软件远程访问服务器桌面的能力。终端服务基本由 3 部分技术组成：客户端部分、协议部分及服务器部分。在客户端安装名为“远程桌面”的程序后，就可以看到服务器完全一致的计算机桌面，并能执行一样的操作。犹如将服务器搬到自己眼前一样。客户端和服务器通过远程桌面协议进行通信。

在 Windows Server 2008 R2 中，终端服务也没有被默认安装，需要手动添加。具体步骤为：依次选择“开始”→“管理工具”→“配置您的服务器向导”命令，在打开的“配置您的服务器向导”对话框中，单击“下一步”按钮；按照“预备步骤”窗口中的说明操作，

单击“下一步”按钮；在“服务器角色”对话框，选择“终端服务器”选项，单击“下一步”按钮；按照向导中的说明操作来完成安装。

默认情况下只有系统管理员组用户(Administrators)和系统组用户(SYSTEM)拥有访问和完全控制终端服务器的权限，另外远程桌面用户组(Remote Desktop Users)的成员只拥有访问权限而不具备完全控制权。而在很多时候，默认的权限设置往往并不能完全满足实际需求，因此还需要赋予某些特殊用户远程连接的权限。具体操作如下。



图 8.2　“权限”选项卡

依次选择“开始”→“管理工具”→“终端服务配置”命令，在打开的“终端服务配置”对话框中，双击右侧窗格中的“RDP-Tcp”连接。打开“RDP-Tcp 属性”对话框，切换到“权限”选项卡，如图 8.2 所示。“权限”选项卡可以设置有哪些用户和组可以从客户端登录该终端服务器。

2. Windows Server 2008 R2 远程管理

远程管理的使用与活动目录和组策略的使用一样重要，是衡量 Windows Server 2008 R2 网络管理员、系统管理员水平的重要指标。

在 Windows Server 2008 R2 家族操作系统中，进行远程管理的方法是多种多样的，主要包括 MMC(微软管理控制台)法、远程桌面连接法、管理远程桌面(终端服务)法、管理工具方法、远程协助法、Telnet 法、远程管理 Web 法和远程存储法。

1)　Microsoft 管理控制台(MMC)

Microsoft 管理控制台集成了用来管理网络、计算机、服务及其他系统组件的管理工具。但 MMC 不执行管理功能，可以使用 MMC 创建、保存并打开管理工具单元，这些管理工具用来管理软件、硬件和 Windows 系统的网络组件。

使用 MMC 有以下两种方法。

(1)　在用户模式中使用已有的 MMC 控制台管理系统。

(2)　创建新控制台或修改已有的 MMC 控制台。

2)　远程桌面连接

(1)　配置远程桌面连接。

要想成功连接到终端服务器，必须保证服务器允许进行“远程桌面”连接。右击“我的电脑”图标，在弹出的快捷菜单中选择“属性”命令，打开“远程”选项卡，勾选“允许用户远程连接到您的计算机”复选框。

(2)　使用桌面连接。

用户要想远程连接到终端服务器，首先需要安装客户端。安装完客户端后执行以下操作就可以连接到终端服务器。



图 8.3　运行远程访问服务

依次选择“开始”→“所有程序”→“附件”→“远程桌面连接”命令，在打开的“远程桌面连接”对话框中，单击“选项”按钮，切换到详细的登录对话框，如图 8.3



所示。输入终端服务器的 IP 地址、用户名、密码，并单击“连接”按钮。出现 Windows 登录对话框后输入已授权的用户名的密码即可完成连接。

8.2.2 Red Hat Enterprise Linux 7

8.2.2.1 Red Hat Enterprise Linux 简介

Linux 发行版本趋于多样化。目前在操作系统核心(Kernel)部分，常用的版本是 4.x.x。为了方便安装，将操作系统核心与各种软件组合起来一起包装，作为 Linux 的发行版本，目前市场上已经有 300 多种发行版本，如 Red Hat Linux、Slackware Linux、Open Linux、Informagic、SuSE Linux、Debian Linux、Redflag Linux、Turbo Linux、Linux-Mandrake 和红旗 Linux 等。

Red Hat 于 2014 年 6 月 9 日正式发布 Enterprise Linux 7 以来，已经更新至 Enterprise Linux 7.3 版本。该版本内核为 Kernel 3.10，它在 RHEL 6 的基础上又有了很大的改进，集成了应用程序虚拟化技术 Docker 和对 systemd 进程管理器的支持，XFS 成为 RHEL 7 默认的文件系统以及能监控系统 PCP 等新功能特性，使之较 RHEL 6 在功能和性能方面有很大提升。

8.2.2.2 Red Hat Enterprise Linux 7 的安装

Red Hat Enterprise Linux 7 图形化安装程序引入了一个全新的用户界面设计，使安装方便、快捷。新的安装程序界面将一组配置选项放到了一个中心界面，用户单击需要改变的选项，改变它们，然后开始安装。

1. 选择系统引导方式

首先在计算机的 CMOS 中把启动盘的先后顺序设置好，然后把安装光盘放入光驱，重新启动计算机，此时，系统会进行自检，自检完毕后会出现安装系统的引导界面。

这个屏幕包括如下引导选项：

Install Red Hat Enterprise Linux 7.0(安装 RHEL 7.0)

Test this media & install Red Hat Enterprise Linux 7.0(测试安装文件并安装 RHEL 7.0)

Troubleshooting(修复故障)

一般情况下选择第一项，然后按 Enter 键进入引导安装。

2. 配置分区

1) 分区的命名

Linux 通过字母数字的组合来识别硬盘分区。命名规则如下。

前两个字母表示分区所在的设备类型，hd 表示 IDE 硬盘，sd 表示 SCSI 硬盘。

第三个字母表示分区在哪个设备上，hda 表示在第一块 IDE 硬盘上，hdb 表示在第二块 IDE 硬盘上，sdc 表示在第三块 SCSI 硬盘上。

数字表示分区的次序，1～4 表示主分区或扩展分区，逻辑分区从 5 开始。

2) 分区的组织

Linux 系统支持多分区结构，各个分区的功能如表 8.2 所示。

表 8.2　分区功能

分　区	功　能
/	整个系统的基础(必备)
swap	操作系统的交换空间(必备)
/boot	在根下创建，用来单独保存系统引导文件
/usr	用来保存系统软件
/home	包含所有用户的主目录，可保存几乎所有的用户文件
/var	保存邮件文件、新闻文件、打印队列和系统日志文件
/tmp	用来存放临时文件

Linux 系统对分区的基本要求如下。

(1)　至少有一个根分区，用来存放系统文件及程序。其大小至少在 5GB 以上。

(2)　要有一个 SWAP(交换)分区，它的作用相当于 Windows 里的虚拟内存，swap 分区的大小一般为物理内存容量的 1.5 倍(内存<8GB)。当系统物理内存大于 8GB 时，swap 分区配置 8G～16GB 即可，太大无用，浪费磁盘空间。

(3)　/boot 分区，这是 Linux 系统的引导分区，用于存放系统引导文件，所以一般设置 100M～200MB 即可。

这里我们按照企业中最常用到的针对网站集群架构中的某个节点服务器场景进行分区，该服务器上的数据有多分区(其他节点也有)且数据不太重要。

/boot：设置为 200MB。

Swap：物理内存的 1.5 倍，本机内存 8GB，所以设置为 12GB。

/：剩余硬盘空间大小，这就相当于 Windows 中只有一个 C 盘，所有数据和系统文件都放在一起。

8.2.2.3　Red Hat Enterprise Linux 7 的使用

1.　系统启动、关闭等基本操作

1)　启动系统

Red Hat Enterprise Linux 7 是通过 GRUB2 来引导系统的，如果计算机装有多个操作系统，一般只要在 Red Hat Enterprise Linux 7 安装过程中进行了正确的配置，GRUB2 都会在引导界面上显示系统列表，供用户选择进入哪一个系统；如果不选择，系统会在规定的时间后自动进入默认的系统。假如引导系统列表中有多个操作系统，可以通过按下或上键进行选取，选定后按 Enter 键即可。如果是第一次运行该系统，系统将自动进入“欢迎”界面，一般来说，在系统执行自检完成之后，系统将进入 Red Hat Enterprise Linux 7 的登录界面。

2)　用 reboot 命令重新启动计算机

一般情况下，按 Ctrl+Alt+Del 组合键可以重新启动计算机，但是正规的用法是执行 reboot 命令，其语法格式为

```
reboot [-n] [-w] [-d] [-f] [-i]
```

3) 用 shutdown 命令关机或进入单人维护模式

利用 shutdown 命令可以关闭系统中正在运行的所有程序，并可以根据用户的需要进入单人系统维护模式，或执行重开机、关机的操作。shutdown 命令的语法如下。

```
shutdown [-t secs] [-rkhncfF] time [warning message]
```

2. 文本模式和图形化模式的切换

在文本模式下，输入 startx 命令可以直接进入 X Window System 界面。而在 X WindowSystem 界面下，也可以使用文本模式。

Linux 主机在控制台(Console)下提供了 6 个虚拟终端，在每一个虚拟终端中都可以执行各自的程序，如表 8.3 所示。

表 8.3 控制台、组合键和内容

控 制 台	组 合 键	内 叠
1	Ctrl+Alt+F1	X 图形化显示
2	Ctrl+Alt+F2	Shell 提示
3	Ctrl+Alt+F3	安装日志(安装程序的信息)
4	Ctrl+Alt+F4	与系统相关的消息
5	Ctrl+Alt+F5/F6	文本(shell)显示界面
7	Ctrl+Alt+F7	安装提示对话框
1	Ctrl+Alt+F1	X 图形化显示

登录 X Window System 系统后的任何时候，按 Ctrl+Alt+Fn 组合键都可以切换到其他虚拟终端，其中的 Fn 是指 F1 到 F7 功能键。例如，按 Ctrl+Alt+F2 组合键，可切换到第一个虚拟终端；按 Ctrl+Alt+F3 组合键，可切换到第二个虚拟终端；依次类推。若要返回原来的 X Window System 系统界面，可以按 Ctrl+Alt+F1 组合键。

用户也可以在窗口登录界面出现时按 Ctrl+Alt+F7 组合键直接登录文本模式终端。

当然，在 Red Hat Enterprise Linux 7 图形化界面中，通过终端命令程序也可在使用 X Window System 系统的同时使用文本模式。

8.2.2.4 常用命令

1. 目录操作命令

1) 查看目录命令 ls

语法：ls [选项] [目录或是文件]

功能：列出目录的内容。该命令类似于 DOS 下的 dir 命令。默认情况下，输出的条目按字母顺序排序。当未给出目录名或是文件名时，就显示当前目录的信息。

2) 改变工作目录命令 cd

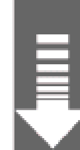
语法：`cd [directory]`

功能：该命令将当前目录改变至 directory 所指定的目录。利用点点(..)把目录上移一级。

3) 创建目录命令 mkdir

语法：`mkdir [选项] dir-name`

功能：创建由 dir-name 命名的目录。该命令类似于 DOS 下的 md 命令。



4)　删除目录命令 rmdir

语法：rmdir [选项] dir-name

功能：删除目录 dir-name。需要特别注意的是，一个目录被删除之前必须是空的。

5)　显示当前目录命令 pwd

语法：pwd

功能：此命令显示出当前工作目录的绝对路径。

2. 文件操作命令

1)　显示文件命令 cat、head、tail、more

(1)　cat 命令。

语法：cat [选项] 文件名

功能：在标准输出上显示指定的文件。如果文件内容很长，在一张屏幕显示不下时，会出现屏幕滚动。

(2)　head 命令。

语法：head [显示行数] 文件名

功能：在屏幕上显示指定文件最前面的若干行，行数由“显示行数”确定。

(3)　tail 命令。

语法：tail [显示行数] 文件名

功能：在屏幕上显示指定文件末尾的若干行，行数由“显示行数”确定。

语法：tail [+n] 文件名

功能：在屏幕上从指定行号 *n* 开始显示，直到文件的末尾。

(4)　more 命令。

语法：more [选项] 文件名

功能：显示文件内容，每次显示一屏，并在屏幕的底部提示已显示的百分比。按 Space 键显示下一屏的内容，按 Enter 键显示下一行的内容，按 B 键显示上一屏的内容，按 Q 键退出 more 命令。

2)　创建新文件命令 touch

语法：touch 文件名

功能：创建空文件夹。

3)　复制文件命令 cp

语法：cp [选项] 源文件或目录 目标文件或目录

功能：把指定的源文件复制到目标文件或把多个源文件复制到目标目录中。该命令同 DOS 下的 copy 命令一样。

4)　移动和重命名文件命令 mv

语法：mv [选项] 源文件或目录 目标文件或目录

功能：为文件或目录改名或将文件由一个目录移到另一个目录中。当第二个参数类型是文件时，mv 命令完成文件重命名；当第二个参数是已存在的目录名称时，源文件或目录参数可以有多个，mv 命令将各参数指定的源文件均移至目标目录中。

5)　删除文件命令 rm

语法：rm [选项] 文件

功能：删除不需要的文件和目录。对于链接文件，只是断开了链接，原文件保持不变。

6) 文件链接命令 ln

语法：ln 源文件 目标文件

功能：在文件间建立链接。如果目标文件是到某一目录文件的目录，源文件会链接到此目录下，文件名不变；如果目标文件不是到某一目录文件的路径，源文件会链接到此目标文件，并覆盖已经存在的同名文件。

7) 文件内容比较命令 diff 和 cmp

(1) diff 命令。

语法：diff 文件1 文件2 …

功能：用于比较文本文件，并显示两个文件的不同。

(2) cmp 命令。

语法：cmp 文件1 文件2 …

功能：用于比较数据文件，只报告从哪一个字节开始出现不同。

8) 查找命令 find 和 locate

(1) find 命令。

语法：find 路径名 [选项]

功能：查找文件和目录的位置。

(2) locate 命令。

语法：locate 文件名 [选项]

功能：用于文件和目录的查找。使用 locate 命令的前提是要首先创建一个用于定位文件或目录位置的 slocate 数据库，而且该数据库应是时时更新的，这样才能保证 locate 查找结果的准确性。

9) 文件中查找正文命令 grep

语法：grep [选项] 查找模式 文件名

功能：在文件中查找指定模式的词或短语，并在标准输出上显示包括给定字符串的所有行。

3. 文件权限操作命令

Linux 系统中的每个文件和目录都有访问许可权限，用来确定谁可以通过何种方式对文件和目录进行访问和操作。

1) 改变文件属主命令 chmon

语法：chmon [选项] 用户或组文件

功能：更改某个文件或目录的所有权。用户可以是用户名或用户 ID，组可以是组名或组 ID。文件是以空格分开的要改变权限的文件列表、文件参数。

2) 改变用户组命令 chgrp

语法：chgrp [选项] group 文件名

功能：改变文件或目录所属的组。其中 group 可以是用户组 ID，也可以是/etc/group 文件中用户组的组名。文件名是以空格分开的要改变目录所在的文件列表，支持通配符。如果用户不是该文件的属主或超级用户，则不能改变该文件的组。



3)　chmod

语法：chmod key 文件名

功能：改变文件或目录的访问权限。只有文件主或超级用户 root 才有权用 chmod 命令改变文件或目录的访问权限。

提示： 访问权限规定了 3 种不同类型的用户，分别是文件属主(owner)、同组用户(group)和可以访问系统的其他用户(others)。每类用户有 3 种访问方式，即可读(r)、可写(w)、可执行或查找(x)。如图 8.4 所示的文件权限表示，该文件的属主有可读、可写和可执行权力，而同组用户和其他用户只有可读和可执行权力。文件权限也可以由 3 个八进制数来表示，例如，上述文件权限可表示为 755。

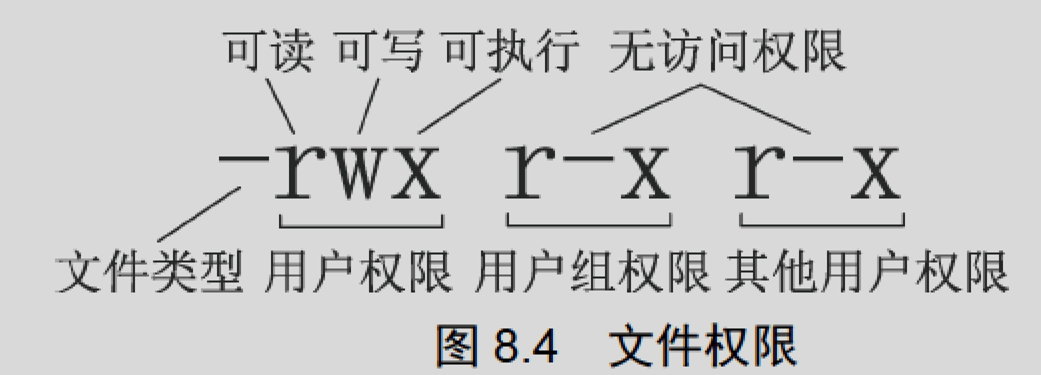


图 8.4　文件权限

4. 进程和作业控制命令

1)　ps 命令

语法：ps [option [arguments] …]

功能：观察进程状态，把当前瞬间进程的状态显示出来。

2)　top 命令

功能：用于读入计算机系统的信息，包括当前的系统数据和进程的状态等。

3)　kill 命令

功能：用于终止进程的执行，释放进程占用的系统资源。

4)　at 命令

语法：at [选项] 时间[日期]

功能：在指定的时间运行用户安排的作业。

5. 基本网络命令

1)　telnet 命令

语法：telnet [选项] IP 地址/主机名

功能：用于远程登录。成功连接远程计算机后，telnet 就显示登录信息，提示用户输入注册名和口令。

2)　ping 命令

语法：ping [选项] IP 地址/主机名

功能：用来确定网络上的主机是否可到达和到达速率。

3)　inger 命令

语法：fing [选项] 用户@主机名

功能：查询系统用户的信息，显示某个用户的用户名、主目录、停滞时间、登录时间等信息。

8.2.3 Windows Server 2008 R2 IIS 服务的配置

8.2.3.1 IIS 服务器的基本概念

在组建局域网时，可以利用因特网信息服务器(Internet Information Server，IIS)来构建WWW 服务器、FTP 服务器和 SMTP 服务器等。IIS 服务提供了一个功能全面的软件包，面向不同的应用领域给出了 Internet/Intranet 服务器解决方案。在 Windows Server 2008 R2 中集成了 IIS 7.5，在 IIS 7.5 模块化的基础上，增强了管理模块，扩充了功能，开始支持 ASP.NET、更多的 PowerShell 命令行和集成 WebDAV 等。

1. WWW 服务

WWW(World Wide Web)是图形最为丰富的 Internet 服务。Web 具有很强的链接能力，支持协作和工作流程，可以给分布在世界各地的用户提供商业应用程序。Web 是 Internet 上主机的集合，使用 HTTP 协议提供报文传输服务。基于 Web 的信息使用超文本标记语言，以 HTML 格式传送，它不但可以传送文本信息，还可以传送图形、图像、动画、声音和视频信息。这些特点使得 WWW 成为遍布世界的信息交流平台。

2. FTP 服务

文件传输协议(File Transfer Protocol，FTP)是在 Internet 中两个远程计算机之间传送文件的协议。该协议允许用户使用 FTP 命令对远程计算机中的文件系统进行操作。通过 FTP 可以传送任意类型、任意大小的文件。Windows Server 2008 R2 中 IIS 7.5 里内置了 FTP 模块。

3. SMTP 服务

简单邮件传输协议(Simple Mail Transfer Protocol，SMTP)在客户机应用程序和远程计算机的邮件服务器之间传送邮件信息。也可以通过配置域控制器，使之利用 SMTP 服务跨越站点上的链接实现邮件复制功能。

4. POP3 服务

邮局协议(Post Office Protocol，POP)第 3 版是目前使用最广泛的邮件服务。POP3 的功能是邮件的存储和管理，能为用户提供账号、密码和身份验证功能，与 SMTP 服务配合，提供完整的邮件服务。

8.2.3.2 安装 IIS 服务

IIS 中集成了多种服务，除了可提供 Web 服务外，还提供用于文件传输的 FTP(文件传输协议)服务、用于邮件服务的 SMTP(简单邮件传输协议)服务和用于新闻组的 NNTP(网络新闻传输协议)服务。Windows Server 2008 R2 中集成了最新的 IIS 7.5，IIS 7.5 包含了 Web 服务器和 FTP 服务器。

下面介绍 IIS 7.5 的安装方法。

(1) 选择【开始】→【管理工具】→【服务器管理器】命令。打开【服务器管理器】窗口后，选择左侧的【角色】节点，在右侧窗格的【角色摘要】部分中单击【添加角色】

超链接，启动添加角色向导。

(2) 在【开始之前】向导页中提示此向导可以完成的工作，以及操作之前应注意的相关事项，然后单击【下一步】按钮。

(3) 在【选择服务器角色】向导页中显示所有可以安装的服务器角色，如果角色前面的复选框没有选中，表示该网络服务尚未安装；如果已选中，说明该服务已经安装。 这里选中【Web 服务器(IIS)】复选框，如图 8.5 所示。

(4) 系统提示在安装 Web 服务器(IIS)角色时，必须安装 Windows 进程激活服务功能，否则无法安装 Web 服务器(IIS)角色，单击【添加必需的功能】按钮，如图 8.6 所示。



图 8.5　选择服务器角色

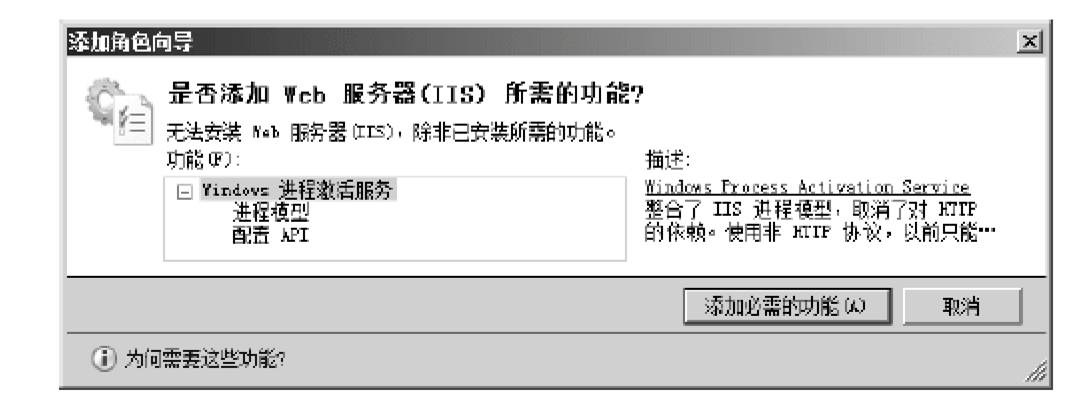


图 8.6　系统提示

(5) 返回【选择服务器角色】向导页后，【Web 服务器(IIS)】复选框被选中，单击【下一步】按钮。

(6) 在【Web 服务器(IIS)简介】向导页中显示 Web 服务器的功能，注意事项和其他信息，单击【下一步】按钮。

(7) 在【选择角色服务】向导页中默认只选择安装 Web 服务所必需的组件，用户可根据实际需要选择安装的组件。例如，Web 服务器需要使用 APS.NET 或 ASP，则需要选中相应的复选框。选择完毕后，单击【下一步】按钮，如图 8.7 所示。

(8) 在【确认安装选择】向导页中显示前面所进行的设置，如果选择错误，用户可以单击【上一步】按钮返回。确认无误后，用户可以单击【安装】按钮开始安装 Web 服务器角色，如图 8.8 所示。

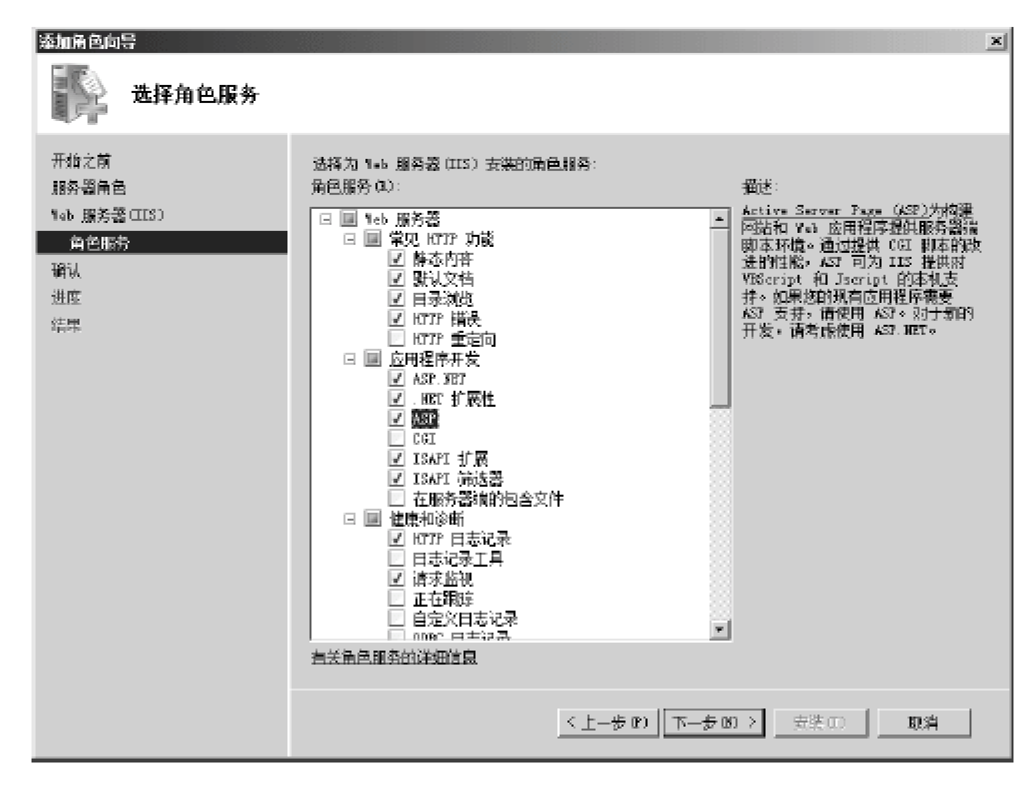


图 8.7　选择角色服务



图 8.8　确认安装选择

(9) 在【安装进度】向导页中显示服务器角色的安装过程。

(10) 在【安装结果】向导页中显示安装 Web 服务器(IIS)角色的已经安装，并列出了已安装的角色服务。单击【完成】按钮关闭【添加角色向导】向导页，即可完成 Web 服务器(IIS)角色的安装。

(11) 基于 IIS 的 Web 服务器安装成功后，用户可以通过【Internet 信息服务(IIS)管理器】窗口来管理 Web 站点。打开【Internet 信息服务(IIS)管理器】窗口的方法是选择【开始】→【管理工具】→【Internet 服务管理器】命令。图 8.9 所示的是【Internet 信息服务(IIS)管理器】窗口，从图中可以看出，在安装 IIS 时已创建一个名为 Default Web Site 的 Web 网站。

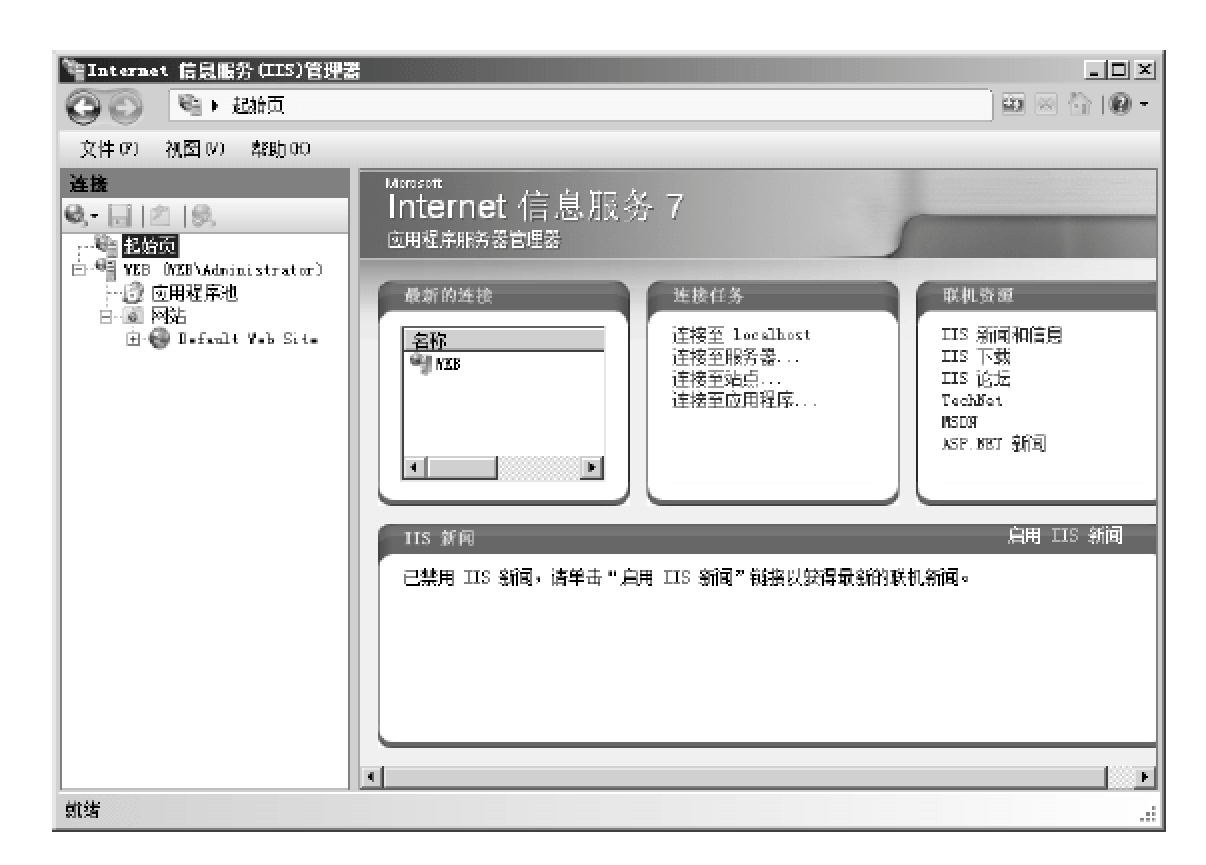


图 8.9 【Internet 信息服务(IIS)管理器】窗口

(12) 在局域网中的另一台计算机上打开浏览器，在地址栏中输入“http://<服务器 IP 或域名>/”，若能看到如图 8.10 所示的界面，则说明 Web 服务器安装成功。



图 8.10 访问 Default Web Site

8.2.3.3 配置 Web 服务器

IIS 7.5 的 Web 服务组件安装成功后，就可以在这台服务器上创建 Web 站点了。默认情况下，在安装的过程中，系统会自动创建一个默认的 Web 站点。用户可以通过修改默认站点的属性发布自己的 Web 网站，也可以重新建立一个 Web 站点。

1. 网站的基本配置

通过“开始”→“管理工具”→“Internet 服务管理器”命令打开“Internet 信息服务(IIS)管理器”对话框。在管理器的左侧窗格中单击“网站”节点前的“+”号，然后选中某个希望配置的网站，右键单击该网站，在弹出的快捷菜单中选择“属性”命令，打开属性对话框。

在“网站”选项卡中可以设置网站的标识，包括网站描述、IP 地址和端口号，还可以设置连接超时、启用日志记录等，从网站日志记录中可以查看哪些用户访问了网站中的哪些内容，如图 8.11 所示。

在 “主目录”选项卡中指定网站 Web 内容的来源，如图 8.12 所示。

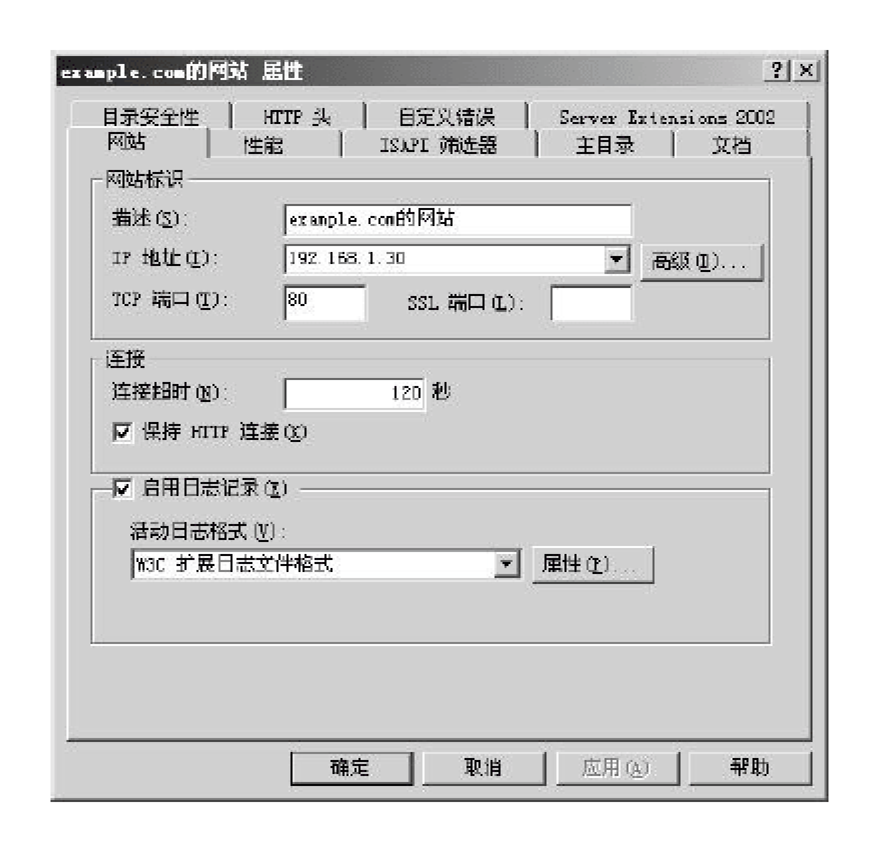


图 8.11　“网站”选项卡



图 8.12　“主目录”选项卡

2. 网站的安全性配置

为了保证 Web 网站和服务器的安全，可以在“目录安全性”选项卡上为网站进行身份验证和访问控制、IP 地址和域名限制的设置，如图 8.13 所示。在“身份验证和访问控制”选项组中单击“编辑”按钮，打开如图 8.14 所示的“身份验证方法”对话框。使用该对话框可以配置 Web 服务器以验证用户身份。可以验证单个用户或选择用户组来阻止未授权用户与受限制内容建立 Web(HTTP)连接。

选中“启用匿名访问”复选框可以为用户建立匿名连接，此时用户无须专用的账户，而是使用匿名或来宾账户(Guest)登录到 IIS。默认情况下，服务器创建和使用账户 IUSR_计算机名，对应于本书所举的例子，用户名为 IUSR_WIN2008_R2。

如果用户希望对网站的访问者验证身份，也可以在“身份验证方法”对话框中的“用户访问需经过身份验证”选项组中进行设置。在此部分中选中的选项要求用户在访问服务器上的任何信息前，提供有效的 Microsoft Windows 用户名和密码。当前 IIS 7.5 中提供了以下 3 种身份验证方法。

① 基本身份验证。用户使用基本身份验证访问 Web 站点时，系统会模仿为一个本地用户(即能实际登录到 Web 服务器的用户)登录到 Web 服务器，因此用于基本验证的 Windows 用户必须具有“本地登录”用户权限。它是一种工业标准的验证方法，大多数浏览器支持这种验证方法。在使用基本身份验证方法时，用户密码是以未加密形式在网络上传输的，很容易被蓄意破坏系统安全的人在身份验证过程中使用协议分析程序破译用户和密码，因此这种验证方式是不安全的。




图 8.13 “目录安全性”选项卡

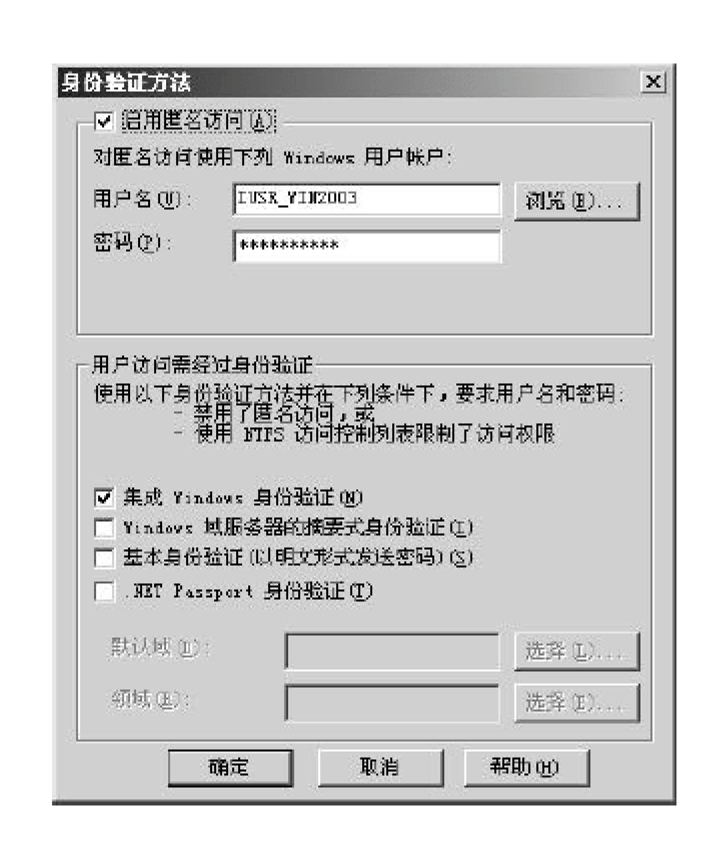


图 8.14 “身份验证方法”对话框

② 摘要式身份验证。摘要式身份验证也要求用户输入账号名称和密码，但账号名称和密码都经过 MD5 算法处理，然后将处理后产生的散列随机数(Hash)传送给 Web 服务器。采用这种方法时，Web 服务器必须是 Windows 域的成员服务器。

③ Windows 身份验证。集成 Windows 验证是一种安全的验证形式，它也需要用户输入用户账户和密码，但账户名和密码在通过网络发送前会经过散列处理，因此可以确保其安全性。Windows 身份验证方法有两种，分别是 Kerberos v5 验证和 NTLM，如果在 Windows 域控制器上安装了 Active Directory 服务，并且用户的浏览器支持 Kerberos v5 验证协议，则使用 Kerberos v5 验证，否则使用 NTLM 验证。

Windows 身份验证优先于基本身份验证，但它并不先提示用户输入用户名和密码，只有 Windows 身份验证失败后，浏览器才提示用户输入用户名和密码。虽然 Windows 身份验证非常安全，但是在通过 HTTP 代理连接时，Windows 身份验证不起作用，无法在代理服务器或其他防火墙应用程序后使用。因此，Windows 身份验证最适合企业 Intranet 环境。

用户可以基于 IP 地址或域名来允许或拒绝特定用户、计算机、计算机组或域访问该网站、目录或文件。在图 8.13 所示的“IP 地址和域名限制”选项组中单击“编辑”按钮，打开如图 8.15 所示的“IP 地址和域名限制”对话框。默认情况下，所有的计算机都被允许访问该网站。选中“授权访问”单选按钮，可以授权所有的计算机访问该网站，但在“下列除外”列表框中指定的计算机除外。要添加拒绝访问的计算机、计算机组或域，需单击“添加”按钮，打开如图 8.16 所示的“拒绝访问”对话框，在其中输入希望拒绝计算机的相应信息。输入后，单击“确定”按钮，被拒绝访问的计算机将出现在图 8.15 所示的“下列除外”列表框中。

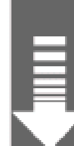


图 8.15 “IP 地址和域名限制”对话框



图 8.16 “拒绝访问”对话框





8.2.3.4　配置 FTP 服务器

Windows Server 2008 R2 中的 IIS 里内置 FTP 服务模块，安装比较简单。在 FTP 服务安装过程中，安装程序会自动创建一个“默认 FTP 站点”，可以直接修改该站点的属性来满足应用需求。为了更好地管理 FTP 服务器，需要对它进行适当的配置。

在 Internet 信息服务控制台下，右键单击“默认 FTP”选项，在弹出的快捷菜单中选择“属性”命令，弹出“默认 FTP 站点 属性”对话框，如图 8.17 所示。对于“FTP 站点”“安全账户”“主目录”和“目录安全性”的设置基本上与 Web 站点相似，这里就不再赘述了。下面着重介绍“消息”选项卡中的相关设置，打开“消息”选项卡，如图 8.18 所示。

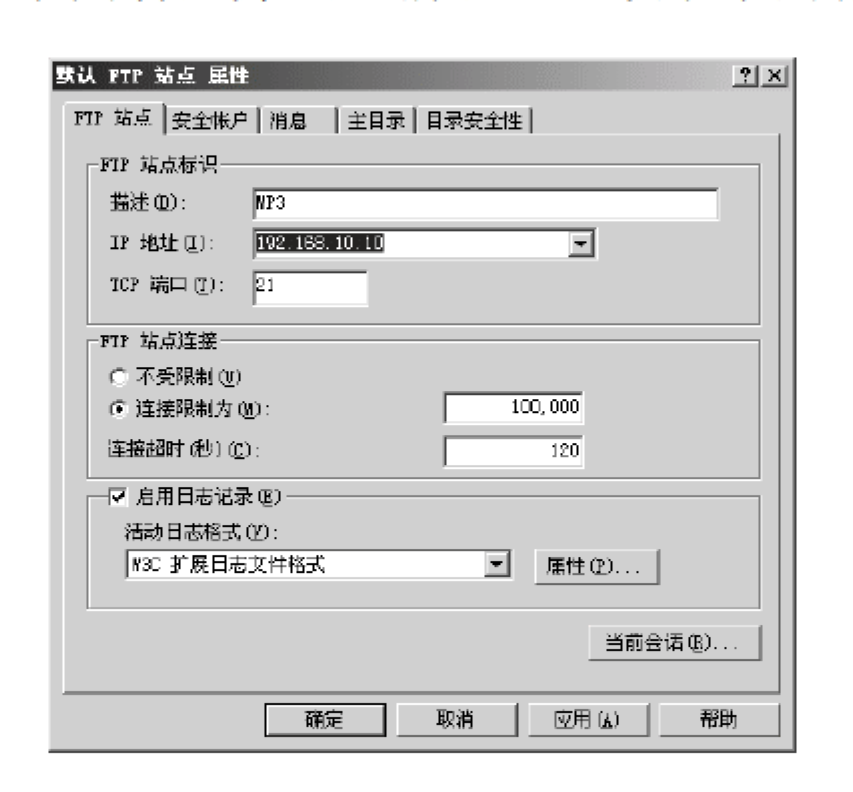


图 8.17　FTP 站点属性



图 8.18　“消息”选项卡

FTP 站点消息的相关设置如表 8.4 所示。

表 8.4　FTP 消息设置

配 置 项	说　明
标题	FTP 的站点名称，用户在登录 FTP 时显示的信息
欢迎	用户登录 FTP 时显示的信息
退出	当用户退出 FTP 时显示的信息
最大连接数	当 FTP 服务器超过最大连接人数时，给提出连接请求的客户机发送一条错误信息

由于服务器配置、性能等的差别，有些服务器不能满足大访问量的需要，往往造成超时甚至死机，因此需要设置连接限制。在图 8.17 所示的“FTP 站点连接”选项组中，有 3 个选项可供选择。

不受限制：该选项允许同时发生的连接数将不受任何限制。

连接限制为：该选项限制允许同时发生的连接数为某一特定值，这一特定值由用户在文本框中输入。

连接超时：当某条 FTP 连接在一段时间内没有反应时，服务器就自动断开该连接。

8.2.3.5　Windows Server 2008 R2 DNS 服务器的安装与配置

1. DNS 服务器的安装

Windows Server 2008 R2 系统内置了 DNS 服务组件，但默认情况下并没有安装，需要

管理员手动安装并配置，从而为网络提供域名解析服务。

在一台运行 Windows Server 2008 R2 的计算机上安装 DNS 服务器的操作步骤如下。

(1) 选择“开始”→“管理工具”→“服务器管理器”→“角色”命令，在打开的窗口中单击“添加角色”按钮，启动 Windows 添加角色向导。

(2) 在“服务器角色”列表框中选中“DNS 服务器”复选框，并单击“下一步”按钮。按照向导提示，执行至确认界面，单击“安装”完成 DNS 服务器的安装。

2. 设置 DNS 服务器

安装完 DNS 服务器后，需要对其进行设置，这样 DNS 服务器才能为客户机提供服务。用于配置和管理 Windows Server 2008 R2 DNS 服务器的主要工具是 DNS 控制台 dnsmgmt。

从“管理工具”窗口中单击 DNS，可以看出 DNS 控制台已默认将本地服务器列在控制台左侧的树中。

假设局域网的域名为 example.com，其中有一台主机作为 WWW 服务器，IP 地址为 192.168.1.30，按照惯例将这台主机命名为 www.example.com。下面介绍如何在 DNS 服务器中实现对该主机名称的解析，步骤如下。

(1) 首先在 DNS 服务器中新建一个名为 example.com 的区域。右键单击控制台目录树中的 EX-WIN2008SVR 服务器，在弹出的快捷菜单中选择“配置 DNS 服务器”命令，打开“配置 DNS 服务器向导”对话框，单击“下一步”按钮。

(2) 在“选择配置操作”对话框中，为了讲解 DNS 服务器的配置，选择“创建正向和反向查找区域”，单击“下一步”按钮。

提示：正向查找区域用于进行 DNS 正向查询，即允许客户端通过已知的主机名，查找其所对应的 IP 地址；反向查找区域用于进行 DNS 反向查询，即允许客户端使用已知的 IP 地址，查找其所对应的计算机名。

(3) 在“新建区域向导”对话框中，由于此时配置的是网络内的第一台 DNS 服务器，所以选中创建“主要区域”单选按钮，单击“下一步”按钮。

(4) 在“区域名称”文本框中输入区域的名称 example.com，如图 8.19 所示，单击“下一步”按钮。

(5) 在“区域文件”界面中，选中“创建新文件，文件名为”单选按钮，并使用系统默认的文件名 example.com.dns，单击“下一步”按钮，如图 8.20 所示。

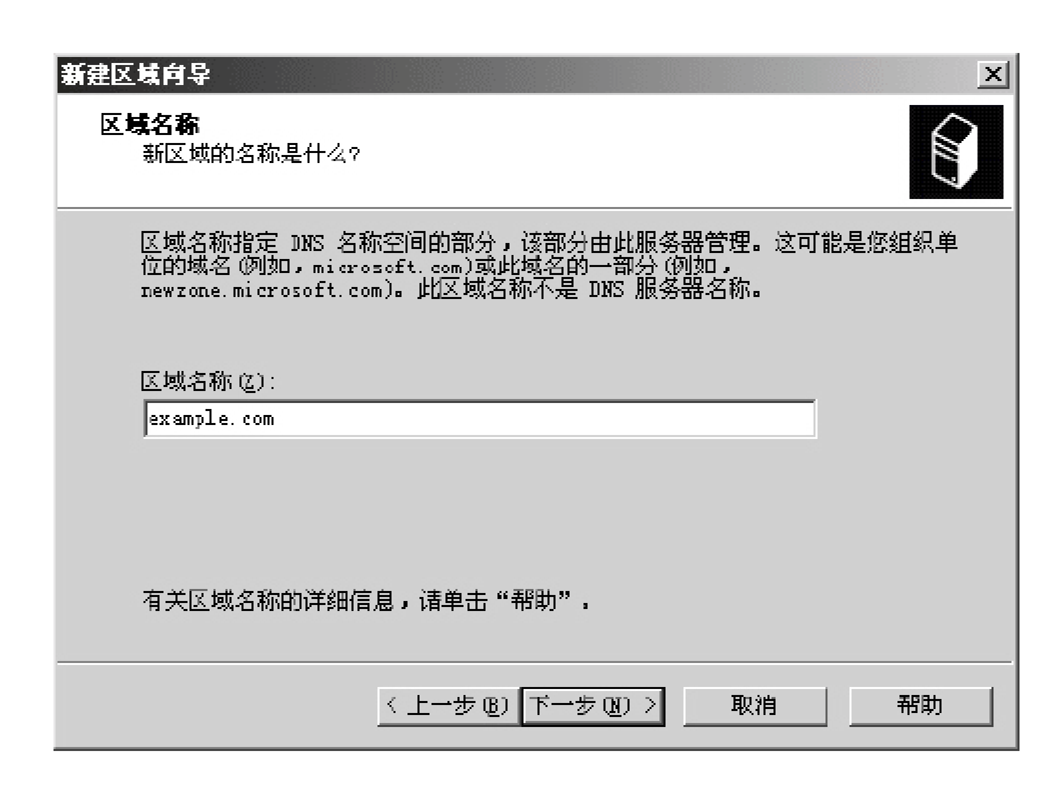


图 8.19　输入区域名称

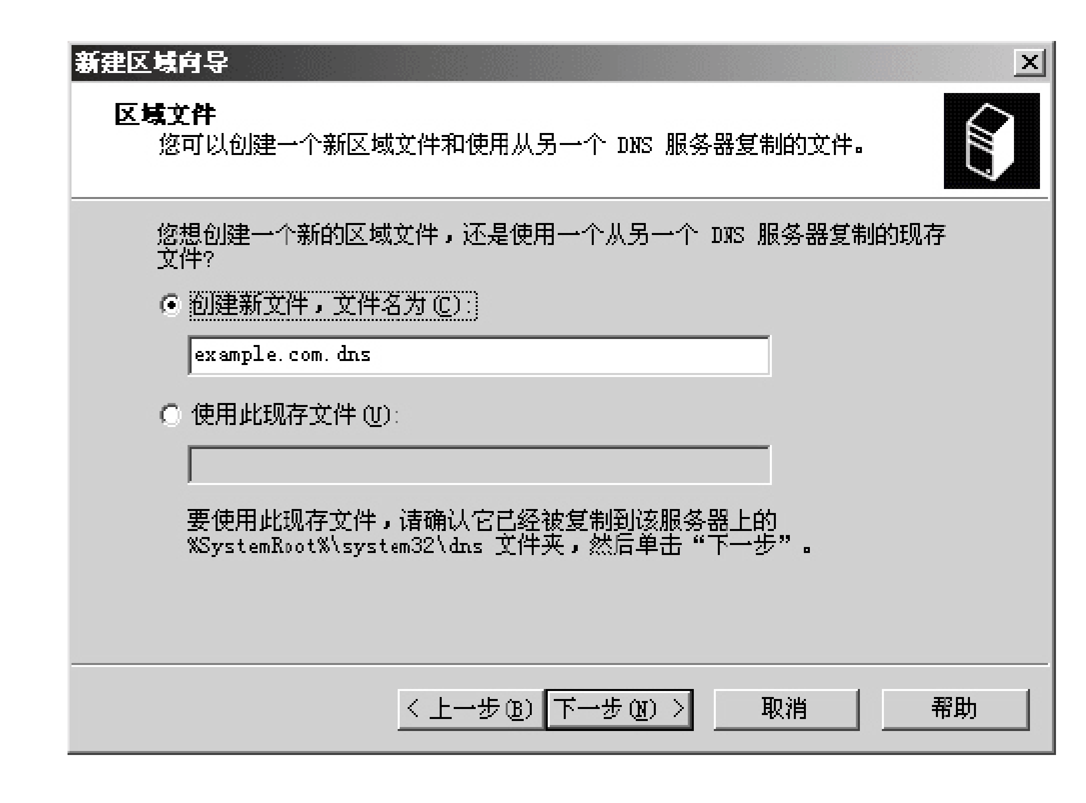


图 8.20　创建新的区域文件



(6) 在“动态更新”界面中，选中“不允许动态更新”单选按钮，如果服务器已安装了 Active Directory，也可以选中“只允许安全的动态更新……”单选按钮，以便最大限度地集成和支持 Active Directory 以及增强的 DNS 服务器功能。单击“下一步”按钮，如图 8.21 所示。

(7) 接下来配置反向区域，在“反向查找区域”界面中，选中“是，现在创建反向查找区域”单选按钮，单击“下一步”按钮。在接下来的“区域类型”界面中，依旧选中“主要区域”单选按钮，再单击“下一步”按钮。

(8) 在“反向查找区域名称”界面中，选中“网络 ID”单选按钮，并在下面输入本网络的网络 ID，如 192.168.1，如图 8.22 所示，单击“下一步”按钮。

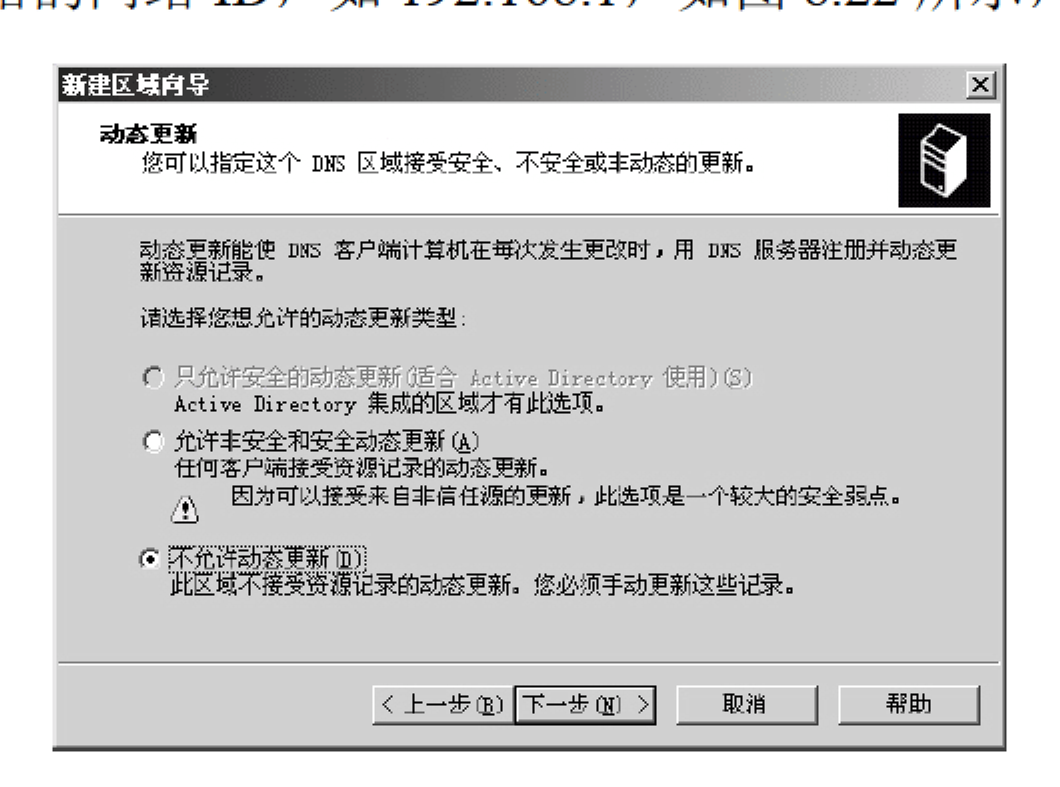


图 8.21　设置 DNS 服务器动态更新类型

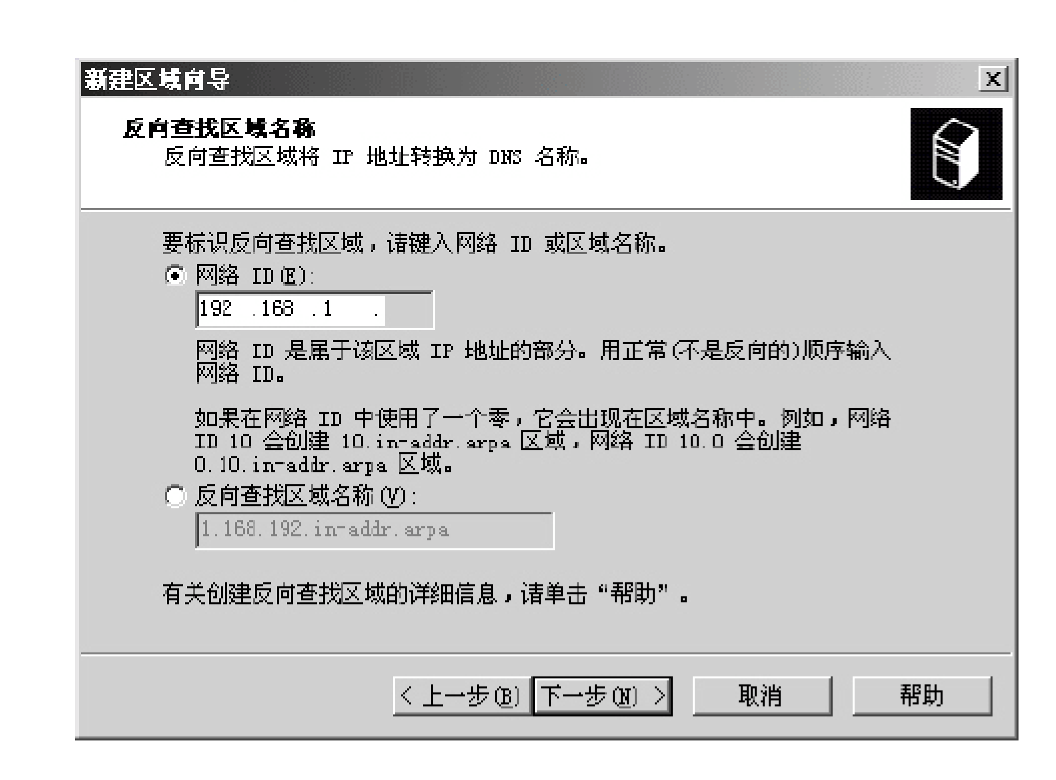


图 8.22　设置反向查找区域名称

(9) 在接下来的“区域文件”和“动态更新”两个界面中，分别选中“创建新文件，文件名为”和“不允许动态更新”单选按钮，文件名按照系统默认给出。

(10) 在“转发器”界面中，暂时选中“否，不向前转发查询”单选按钮。转发器的具体用途和配置方法后面会做进一步介绍。单击“下一步”按钮，如果配置顺利，会弹出一个对话框，提示已成功地完成了 DNS 服务器配置向导，单击“确定”按钮关闭对话框。

DNS 服务器配置完成后，在控制台的目录树中可以看到，服务器节点下建立了“正向查找区域”和“反向查找区域”。双击展开“正向查找区域”，会看到新区域 example.com 已经添加。单击 example.com，右半窗口中会显示该区域的配置信息。

3. 创建域名

下面介绍如何建立主机 www.example.com，其操作步骤如下。

(1) 依次选择“开始”→“管理工具”→DNS 命令，打开 dnsmagt 控制台窗口。

(2) 在左侧窗格中依次展开 ServerName→“正向查找区域”目录，然后用鼠标右击区域名处，从弹出的快捷菜单中选择“新建主机”命令，弹出如图 8.23 所示的对话框，输入主机名 www，IP 地址 192.168.1.30。

(3) 如果希望 DNS 服务器也能够进行反向查询，则选中“创建相关的指针(PTR)记录”复选框，单击“添加主机”按钮。如果添加成功，系统会提示“成功地创建了主机记录 example.com。”，如图 8.24 所示，单击“确定”按钮。

(4) 如果不再添加主机，单击“完成”按钮。



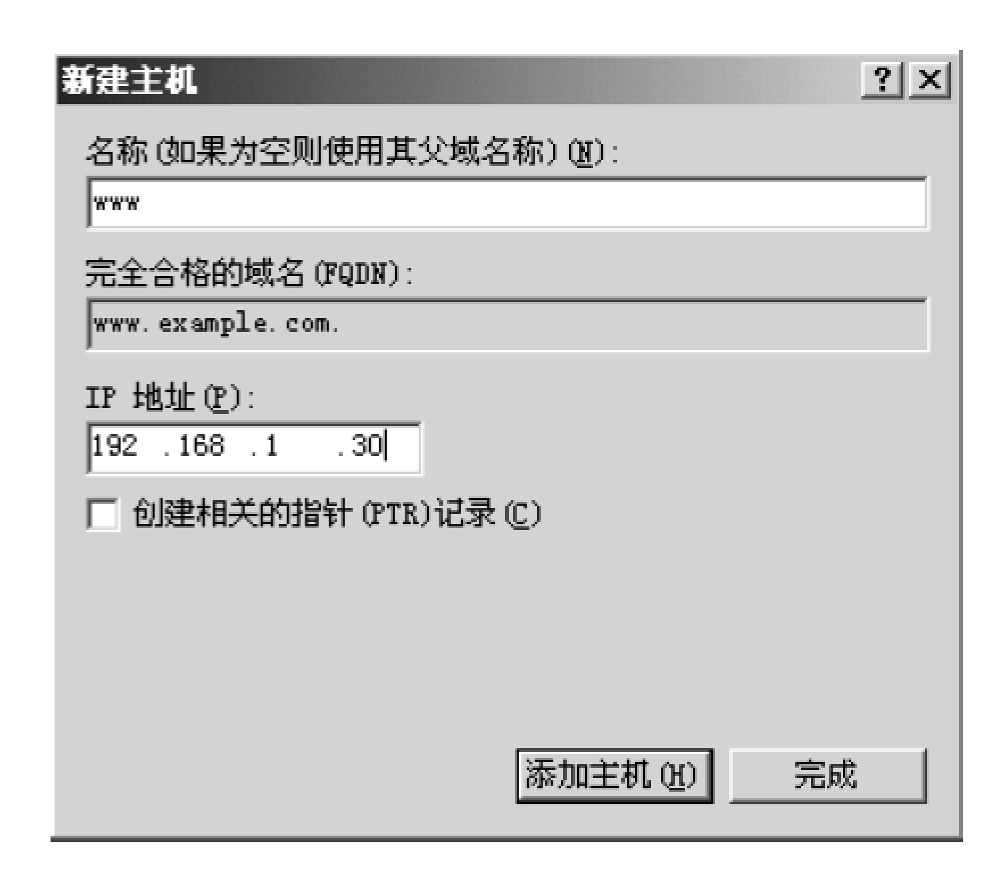


图 8.23 “新建主机”对话框

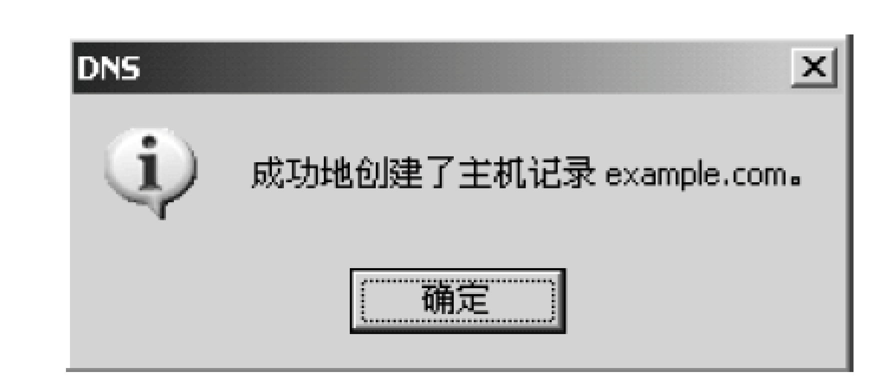


图 8.24 主机记录创建成功

4. 安装客户端

安装 DNS 客户机的步骤如下。

(1) 在“控制面板”对话框中单击“网络和 Internet 连接”图标，打开“网络和 Internet 连接”窗口。

(2) 在“网络和 Internet 连接”窗口中，单击“网络连接”图标，打开“网络连接”窗口。

(3) 右键单击“本地连接”图标，从弹出的快捷菜单中选择“属性”命令，在打开的“本地连接 属性”对话框中选中“Internet 协议(TCP/IP)”复选框，单击“属性”按钮，打开如图 8.25 所示的对话框。

(4) 在图 8.25 的“首选 DNS 服务器”文本框中输入一台 DNS 服务器的 IP 地址，然后单击“确定”按钮，这样便把该计算机配置为那台 DNS 服务器的 DNS 客户机了。

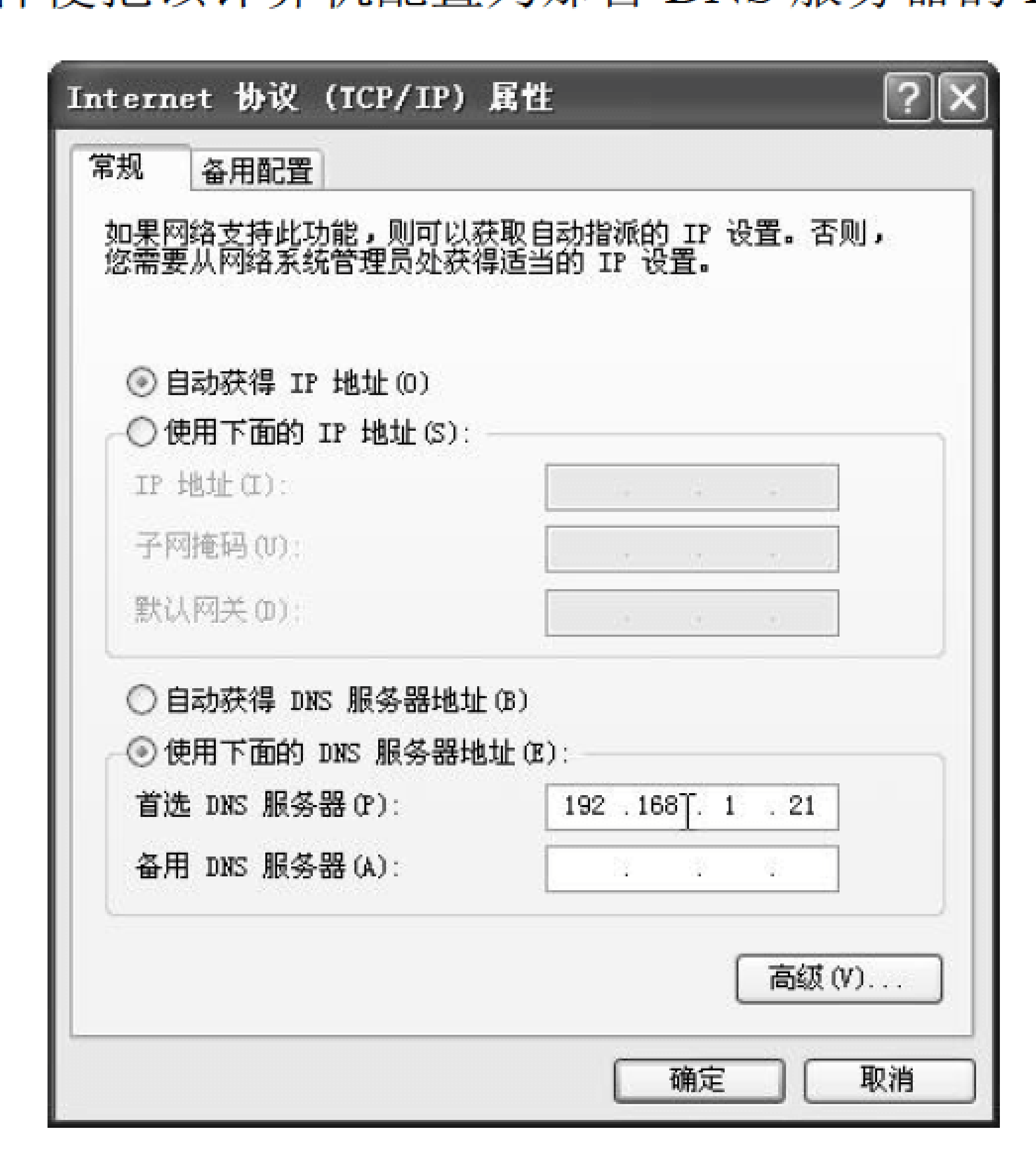


图 8.25 “Internet 协议(TCP/IP)属性”对话框



8.2.3.6　Windows Server 2008 R2 DHCP 服务器的安装与配置

1. 安装 DHCP 服务器

Windows Server 2008 R2 系统内置了 DHCP 服务组件，但默认情况下并没有安装，需要管理员手动安装并配置，从而为网络提供 DHCP 服务。将一台运行 Windows Server 2008 R2 的计算机配置成 DHCP 服务器，最简单的方法是使用服务器管理器添加 DHCP 服务器角色，其过程如下。

(1) 通过【开始】菜单打开【服务器管理器】窗口，选择左侧的【角色】节点，单击【添加角色】超链接，启动添加角色。

(2) 【开始之前】向导页中提示了此向导可以完成的工作，以及操作之前应注意的相关事项，单击【下一步】按钮。

(3) 【选择服务器角色】向导页中显示了所有可以安装的服务器角色。如果角色前面的复选框没有被选中，则表示该网络服务尚未安装。如果已选中，则说明该服务已经安装。这里选中【DHCP 服务器】复选框，单击【下一步】按钮。

(4) 【DHCP 服务器】向导页中对 DHCP 服务器的功能作了简要介绍，单击【下一步】按钮。

(5) 在【选择网络连接绑定】向导页中选择此 DHCP 服务器将用于向客户端提供服务的网络连接，单击【下一步】按钮，如图 8.26 所示。

(6) 在【指定 IPv4 DNS 服务器设置】向导页中指定客户用于名称解析的父域名，以及客户端用于域名解析的 DNS 服务器 IP 地址，单击【下一步】按钮，如图 8.27 所示。

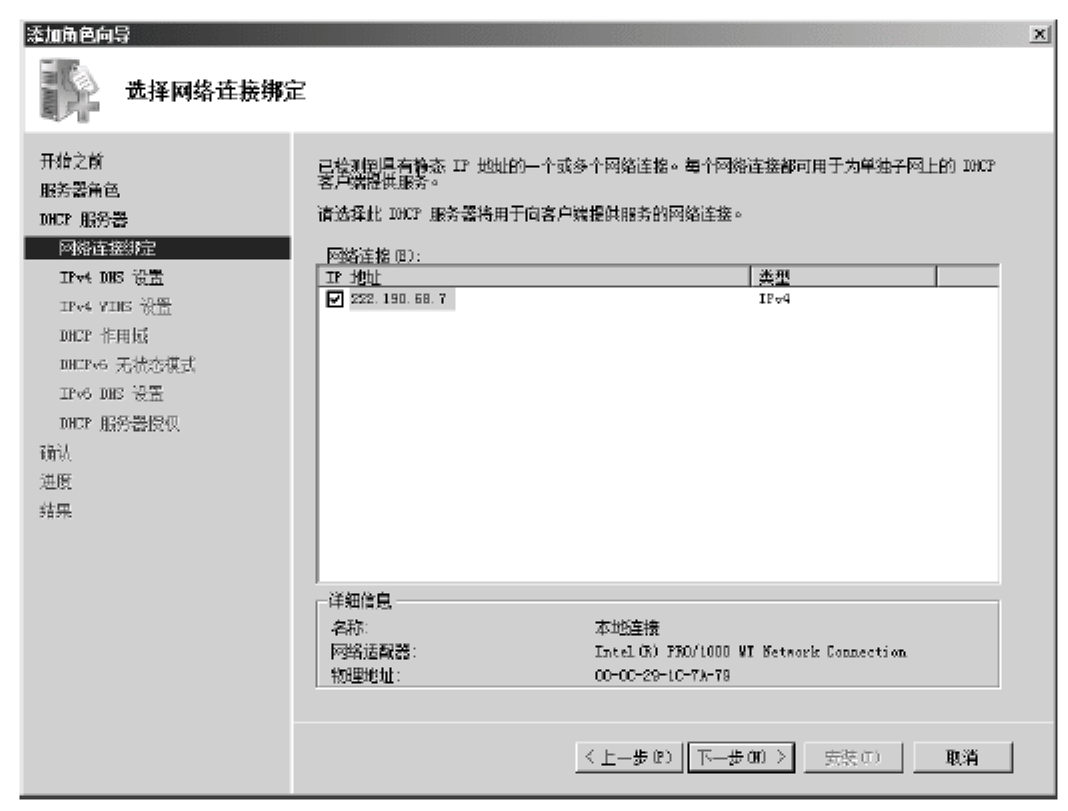


图 8.26　选择网络连接绑定

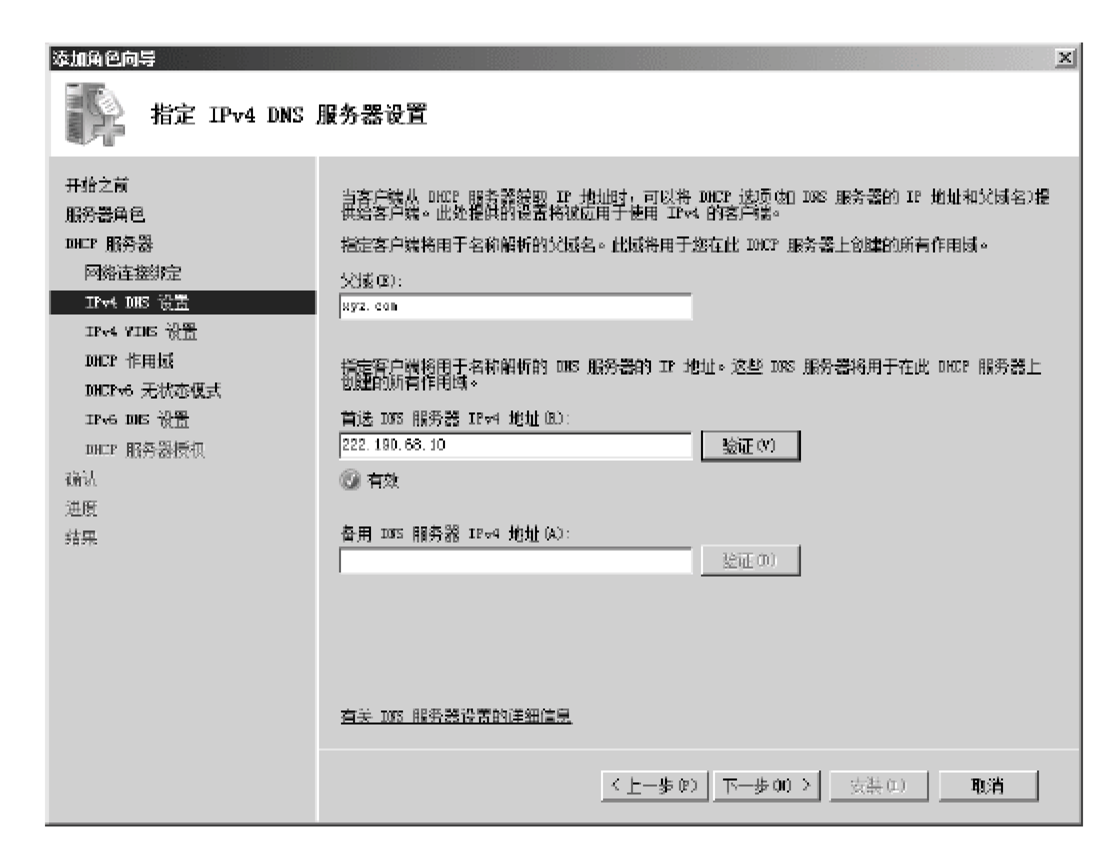


图 8.27　指定 IPv4 DNS 服务器设置

(7) 在【指定 IPv4 WINS 服务器设置】向导页中选择是否使用 WINS 服务，单击【下一步】按钮，如图 8.28 所示。

(8) 在【添加或编辑 DHCP 作用域】向导页中可以添加 DHCP 作用域。只有指定了作用域，DHCP 服务器才能向客户端分配 IP 地址、子网掩码和默认网关等。现在可以不指定，等 DHCP 安装完成后再添加。若现在指定，可单击【添加】按钮，如图 8.29 所示。



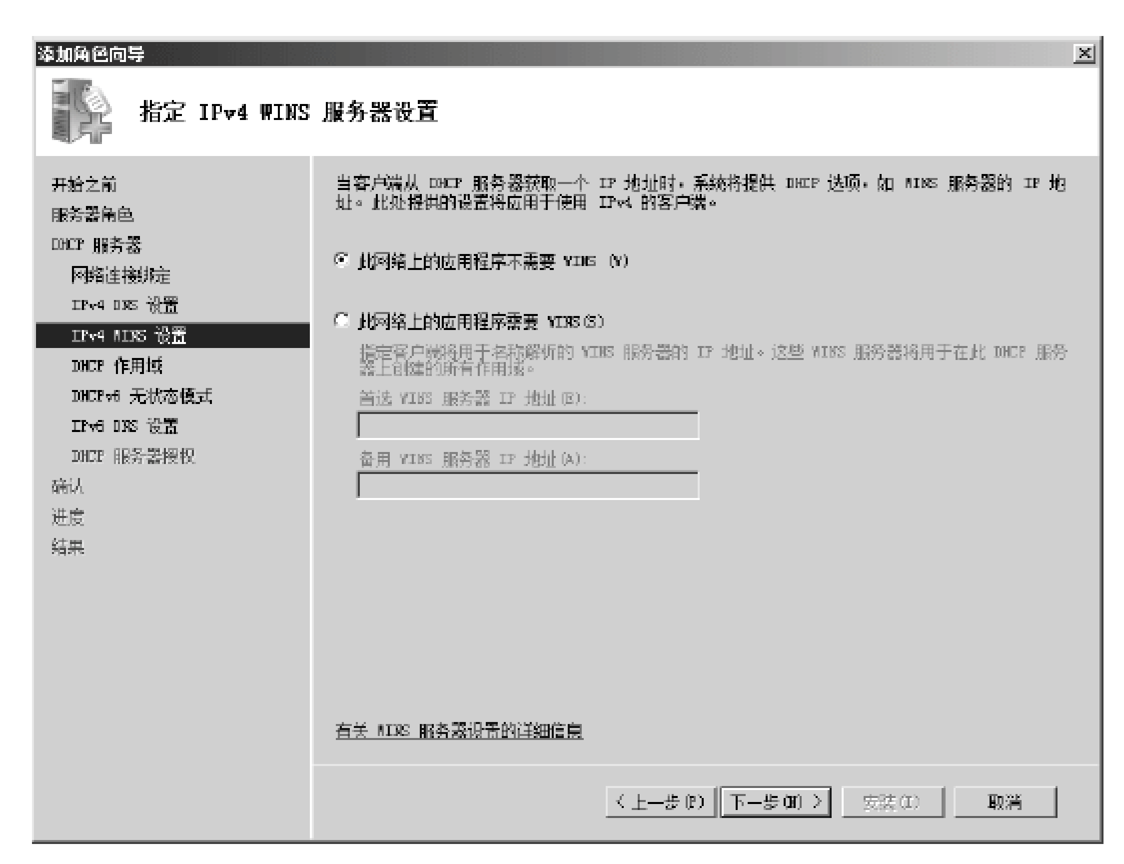


图 8.28　指定 IPv4 WINS 服务器设置



图 8.29　添加或编辑 DHCP 作用域

(9)　在【添加作用域】对话框中设置作用域的名称、起始 IP 地址、结束 IP 地址、子网掩码、默认网关以及子网类型。若选中【激活此作用域】复选框，则创建完成后会自动激活，如图 8.30 所示。设置完成后，单击【确定】按钮，返回上一步操作后单击【下一步】按钮。

(10) 在【配置 DHCPv6 无状态模式】向导页中选择启用还是禁用服务器的 DHCPv6 无状态模式。选中【对此服务器禁用 DHCPv6 无状态模式】单选按钮，单击【下一步】按钮，如图 8.31 所示。

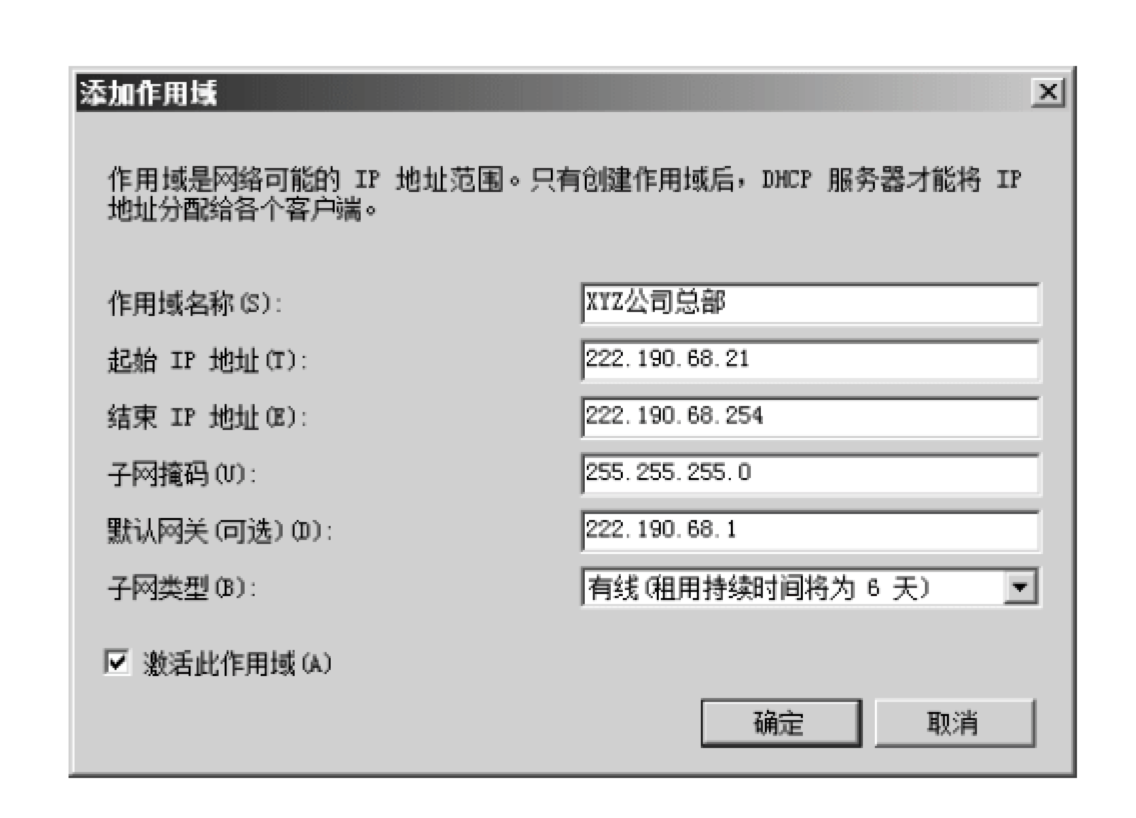


图 8.30　添加作用域



图 8.31　配置 DHCPv6 无状态模式

(11) 若 DHCP 服务器已加入了域，还会打开【授权 DHCP 服务器】向导页，若没有加入域，则不会出现此向导页。为 DHCP 服务器授权必须具有域管理员的权限，若当前没有以域管理员身份登录到域，则选中【使用备用凭据】单选按钮，然后单击【指定】按钮输入域管理员的用户名及密码。单击【下一步】按钮，如图 8.32 所示。

(12) 在【确认安装选择】向导页中，要求确认所要安装的服务器角色及配置情况，如果配置错误，可以单击【上一步】按钮返回。单击【安装】按钮即可开始安装 DHCP 服务器角色，如图 8.33 所示。

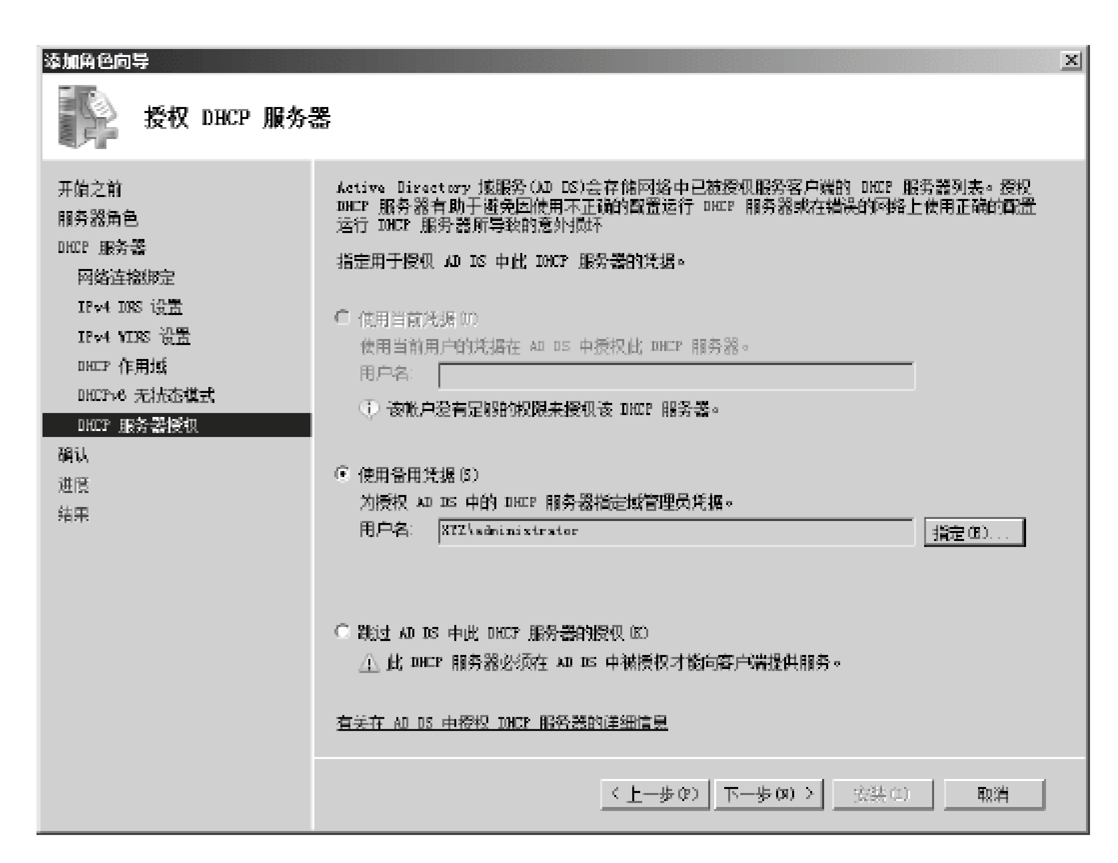


图 8.32　授权 DHCP 服务器

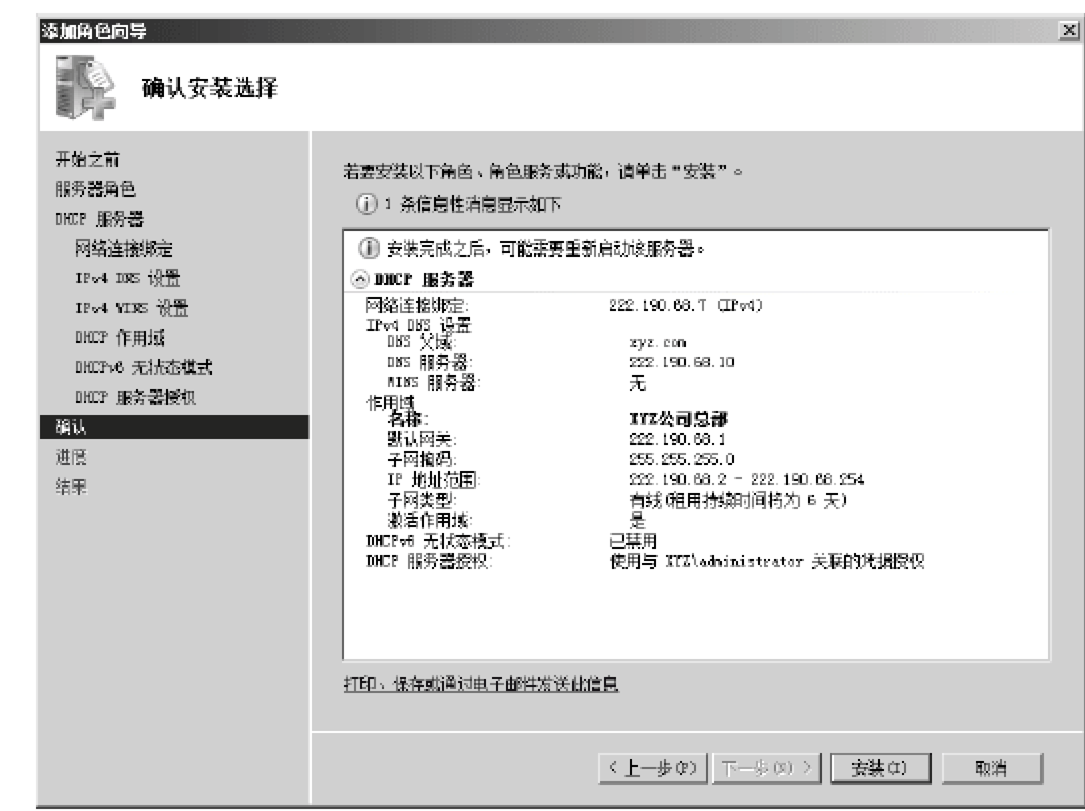


图 8.33　确认安装选择

(13)【安装进度】对话框中显示了安装 DHCP 服务器角色的进度，需耐心等待。

(14)【安装结果】对话框中显示 DHCP 服务器角色已经安装完成，提示用户可以使用 DHCP 管理器对 DHCP 服务器进行配置。若系统未启用 Windows 自动更新，还提醒用户设置 Windows 自动更新，以即时给系统打上补丁。单击【完成】按钮关闭添加角色向导便完成了 DHCP 服务器的安装。

DHCP 服务器安装完毕后，可以通过选择【开始】→【管理工具】→DHCP 命令打开 DHCP 管理器，通过 DHCP 窗口可以管理本地或远程的 DHCP 服务器，如图 8.34 所示。

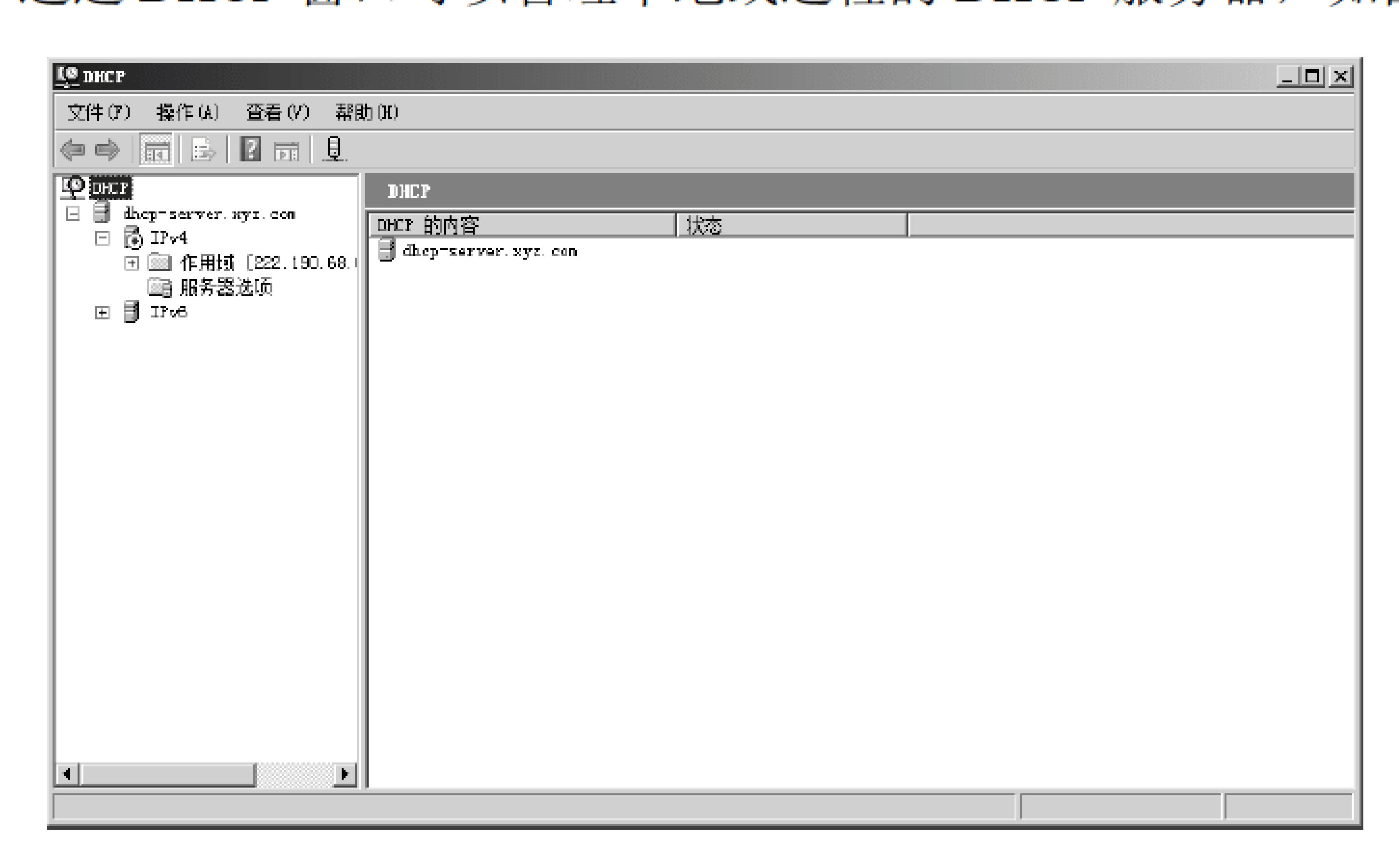


图 8.34　DHCP 管理器

2. 安装 DHCP 客户机

如果希望某台计算机能够自动获取 IP 地址，则需将这台计算机配置为 DHCP 客户机，配置方法如下。

(1) 在“控制面板”中单击“网络和 Internet 连接”图标，打开“网络和 Internet 连接”窗口。

(2) 在“网络和 Internet 连接”窗口中，单击“网络连接”图标，打开“网络连接”窗口。

(3) 右键单击“本地连接”图标，从弹出的快捷菜单中选择“属性”命令，选中“Internet 协议(TCP/IP)”，单击“属性”按钮，打开“Internet 协议(TCP/IP_)属性”对话框。

(4) 选中“自动获得 IP 地址”单选按钮，然后单击“确定”按钮，这样便把该计算机配置为 DHCP 客户机了。

3. 设置 DHCP 服务器

在安装了 DHCP 服务器之后，还需要在 DHCP 服务器上建立一个或多个 IP 地址作用域。“IP 地址作用域”是指可以分配给 DHCP 客户机的 IP 地址范围。这样，当 DHCP 客户机向 DHCP 服务器请求 IP 地址时，DHCP 服务器就可以从 IP 地址作用域中选择一个尚未被租用的 IP 地址，将其分配给 DHCP 客户机。

新建作用域的操作步骤如下。

(1) 依次选择“开始”→“管理工具”→DHCP 命令，打开 DHCP 管理控制台。

(2) 在左侧窗格中，右键单击服务器名，在弹出的快捷菜单中选择“新建作用域”命令。

(3) 在弹出的“新建作用域向导”对话框中单击“下一步”按钮。

(4) 在“名称”文本框中输入一个能够清楚表示该作用域的名称，如图 8.35 所示。

(5) 单击“下一步”按钮，打开设置“IP 地址范围”的界面。地址范围通过设置“起始 IP 地址”和“结束 IP 地址”来指定。通过设置“长度”，用户可以调整子网掩码，以指定 IP 地址中多少位作为网络 ID，多少位作为主机 ID，如图 8.36 所示。



图 8.35 设置作用域名

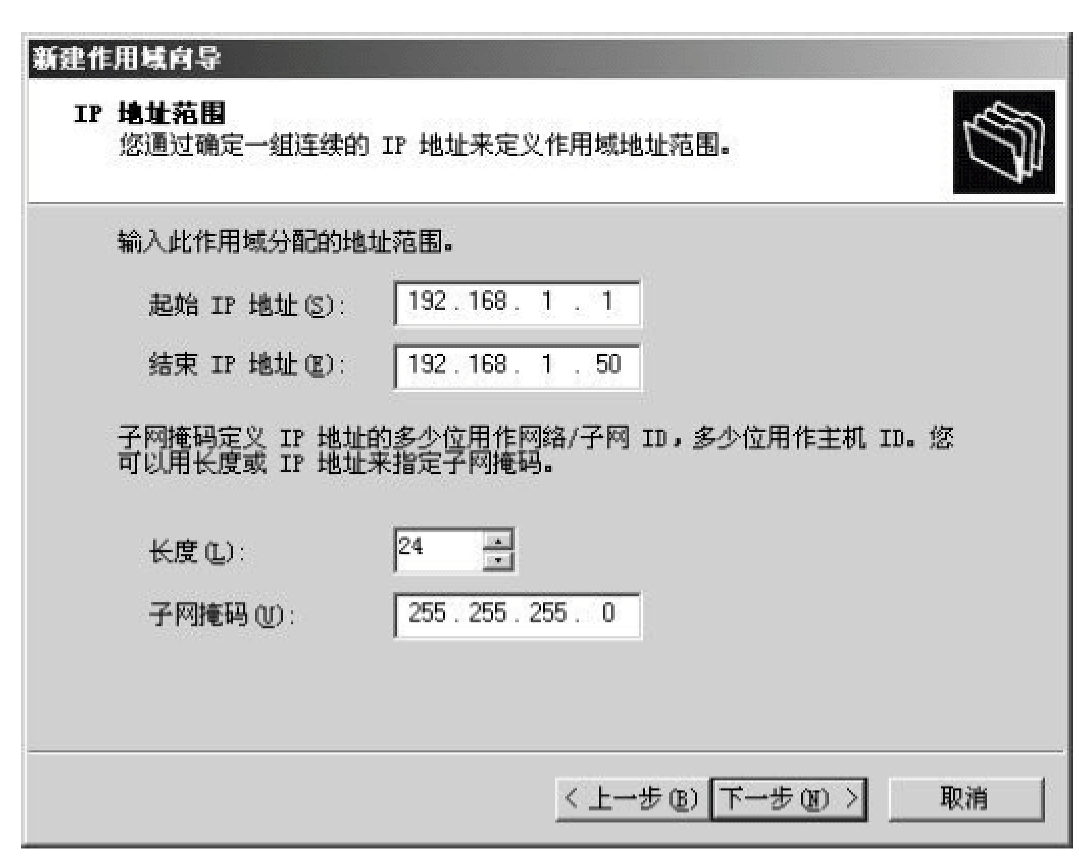


图 8.36 设置 IP 地址范围

(6) 设置好 IP 地址范围后，单击“下一步”按钮，打开“添加排除”界面，如图 8.37 所示。这里用户可以指定前面设置的 IP 地址范围中有哪些地址不被服务器分配。如果想排除的 IP 地址是分散的，那么在“起始 IP 地址”中输入要排除的 IP 地址，然后单击“添加”按钮，重复这一过程直至所有要排除的 IP 地址均被添加。如果想排除的是某一段连续的 IP 地址，则分别输入该范围的起始 IP 地址和结束 IP 地址，然后单击“添加”按钮。

(7) 单击“下一步”按钮，打开“租约期限”界面，如图 8.38 所示。租约期限指的是一个客户端从此作用域使用 IP 地址的时间长短。通常局域网使用的是专用保留 IP 地址，地址数量很充裕，所以可以将租约期限设置得较长。

(8) 单击“下一步”按钮，向导提示用户为该作用域配置 DHCP 选项。通常只有正确配置了 DHCP 选项，DHCP 客户机才可以使用此作用域，所以选中“是，我想现在配置这

些选项”单选按钮。

(9) 单击“下一步”按钮，首先要配置的是默认网关的 IP 地址。输入默认网关的 IP 地址，并单击“添加”按钮。

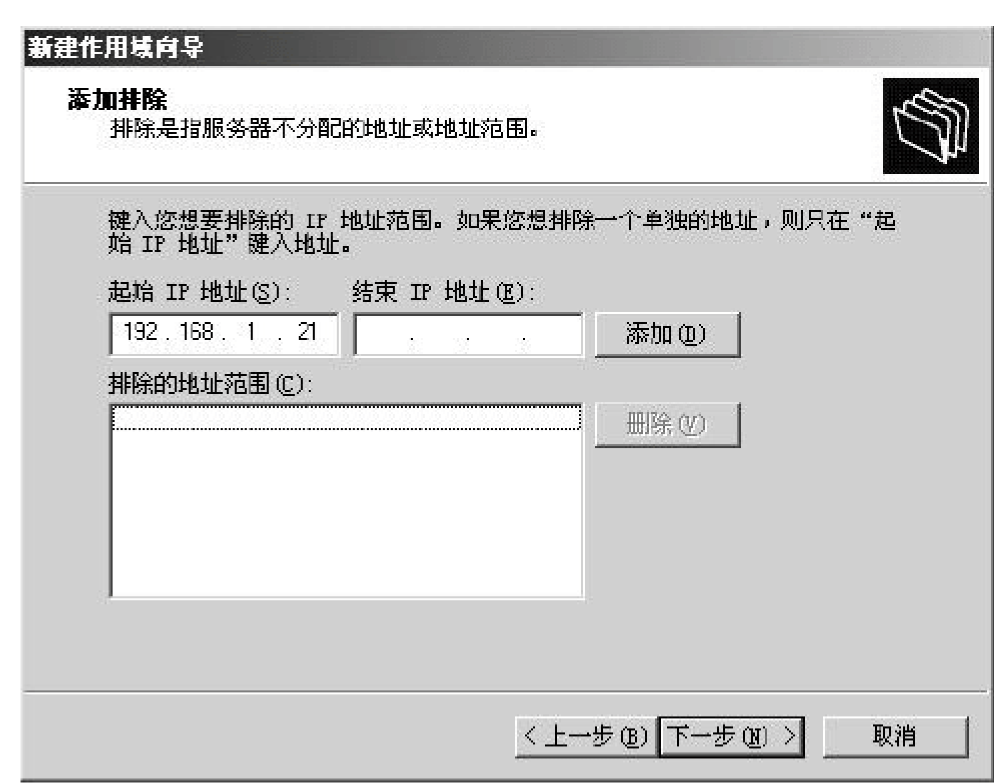


图 8.37　设置排除的 IP 地址

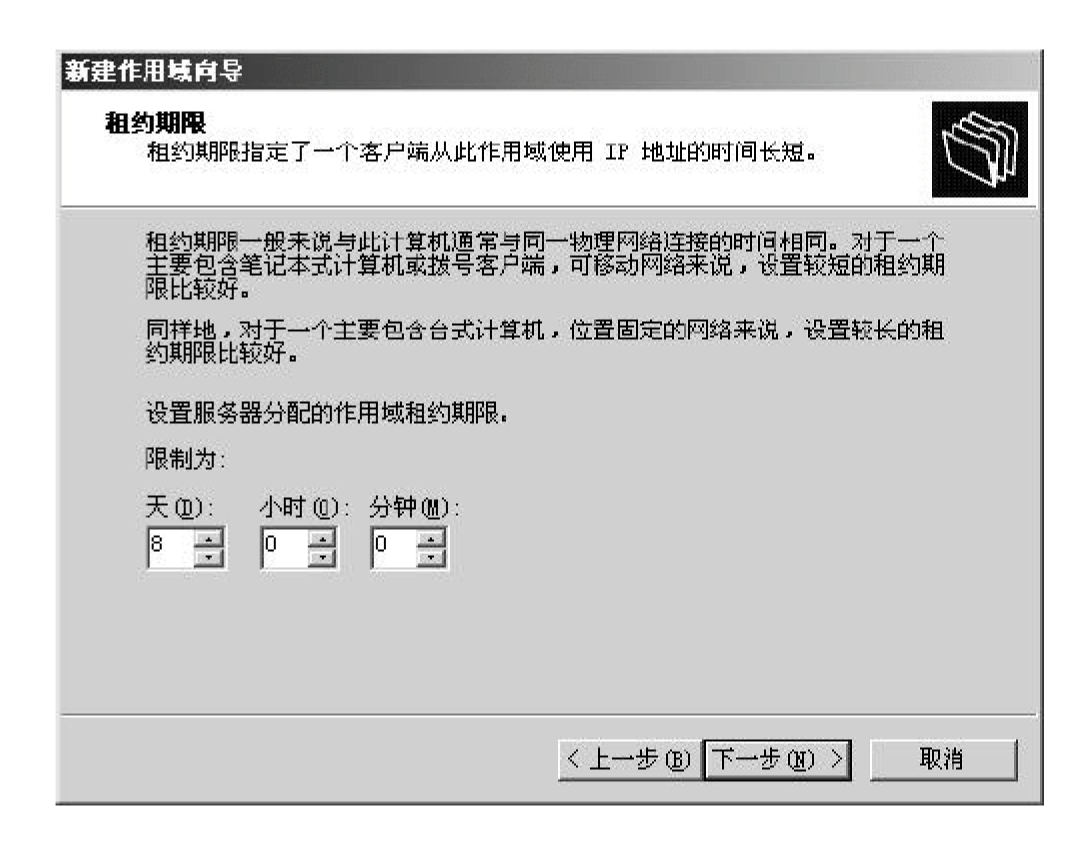


图 8.38　“租约期限”界面

(10) 单击“下一步”按钮，接下来要配置的是域名称和 DNS 服务器。在“父域”文本框中输入域名，并在“IP 地址”文本框中输入 DNS 服务器的 IP 地址，然后单击“添加”按钮，如图 8.39 所示。若有多个 DNS 服务器，将其他的 DNS 服务器添加至此。通常设置两个 DNS 服务器即可，一个作为主 DNS 服务器，另一个作为辅 DNS 服务器。

(11) 单击“下一步”按钮，设置 WINS 服务器地址。如果网络中有 WINS 服务器，在“IP 地址”文本框中输入 WINS 服务器的地址，然后单击“添加”按钮，如图 8.40 所示。

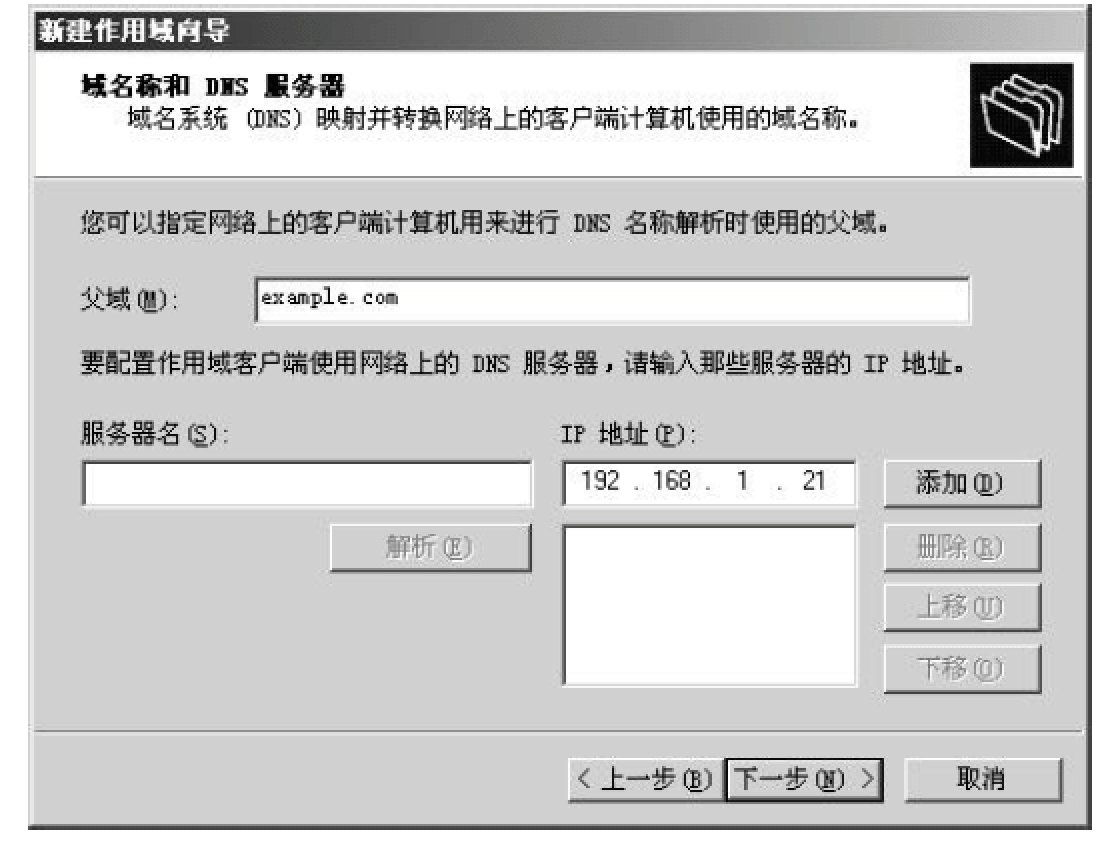


图 8.39　设置域名称和 DNS 服务器

图 8.40　设置 WINS 服务器

(12) 单击“下一步”按钮，向导会提示是否激活此作用域，选择“是，我想现在激活此作用域”。

(13) 单击“下一步”按钮，向导提示已成功完成了新建作用域向导，单击“完成”按钮关闭向导。

接下来，系统会创建新的作用域。创建完成后的控制台如图 8.41 所示。展开新建的作用域，单击“地址池”选项，可以查看当前地址池中 IP 地址的范围及被排除的 IP 地址。单



击“地址租约”选项，可以查看当前有哪些客户端租用了哪些 IP 地址。选择“保留”选项，可以查看并设置将地址池中的某些 IP 地址永久地分配给一些客户端。新建保留地址的方法是右键单击“保留”选项，在弹出的快捷菜单中选择“新建保留”命令，然后在弹出的对话框中输入相应的信息即可。需要注意的是，设置保留地址时，需要知道客户端网卡的 MAC 地址，即物理地址。网卡的物理地址可通过在“命令提示符”中运行 ipconfig /all 命令查看。

单击“作用域选项”选项，可以查看当前为该作用域设置的选项，也就是前面新建作用域向导中所设置的路由器、域名、DNS 服务器和 WINS 服务器等信息。这些是保证客户端能正常访问网络所必需的信息。如果用户还需要为该作用域设置其他的附加选项，可右击“作用域选项”，在弹出的快捷菜单中选择“配置选项”命令，如图 8.42 所示。打开如图 8.43 所示的“作用域 选项”对话框，在“可用选项”中选中要设置的选项，并在下面设置相应的信息，然后单击“确定”按钮即可。

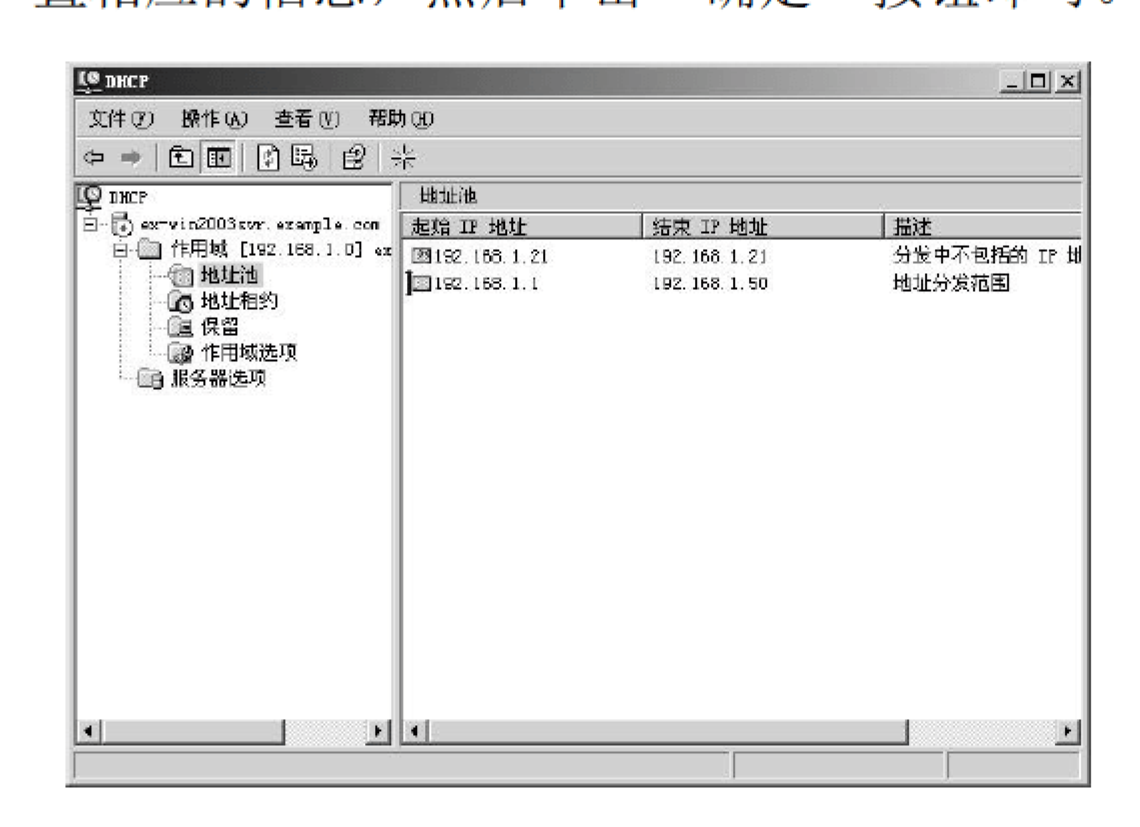


图 8.41　DHCP 服务器的地址池



图 8.42　选择“配置选项”命令

右击新建的作用域，在弹出的快捷菜单中选择“属性”命令，可以对作用域的设置进行更改。作用域的属性对话框共有 3 个选项卡：“常规”、DNS 和“高级”选项卡。

“常规”选项卡如图 8.44 所示，在此可以更改作用域名、IP 地址范围和租约期限。

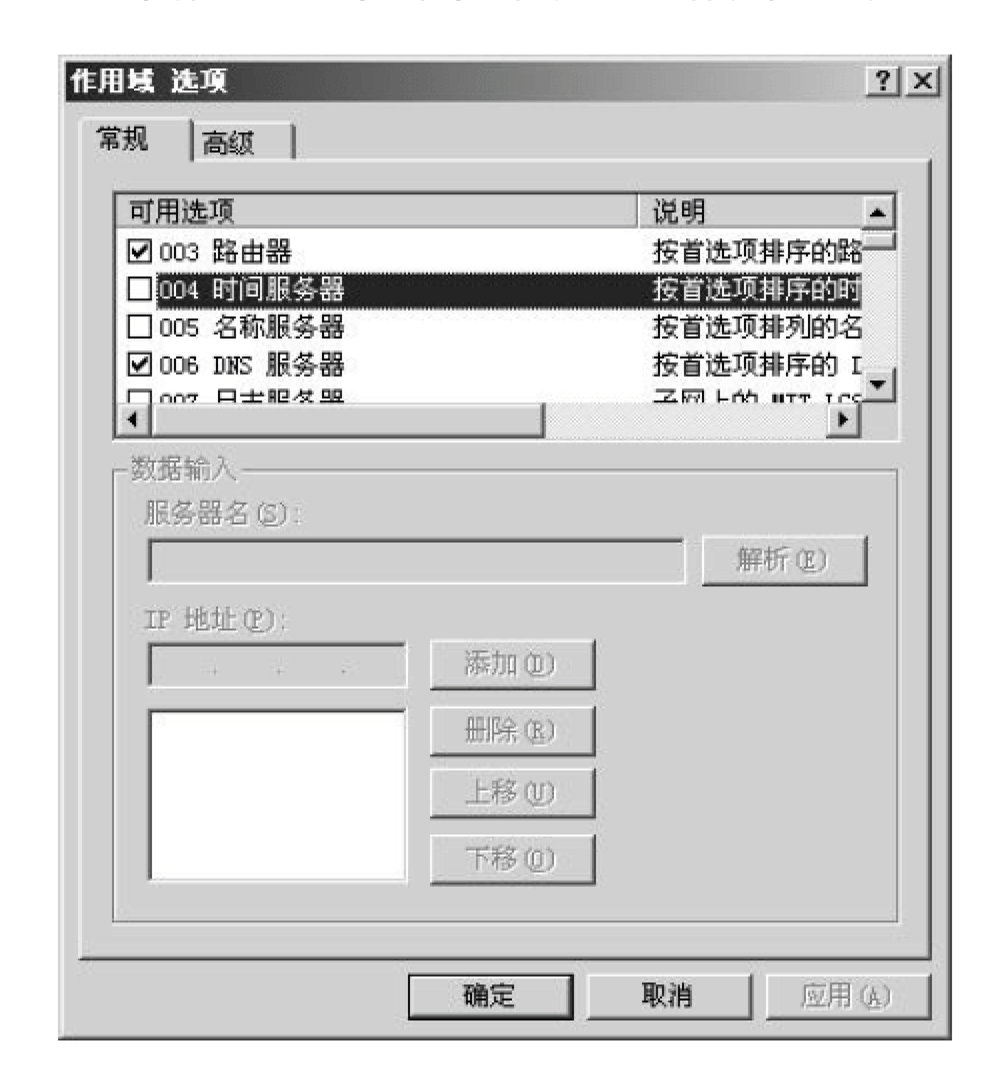


图 8.43　“作用域 选项”对话框

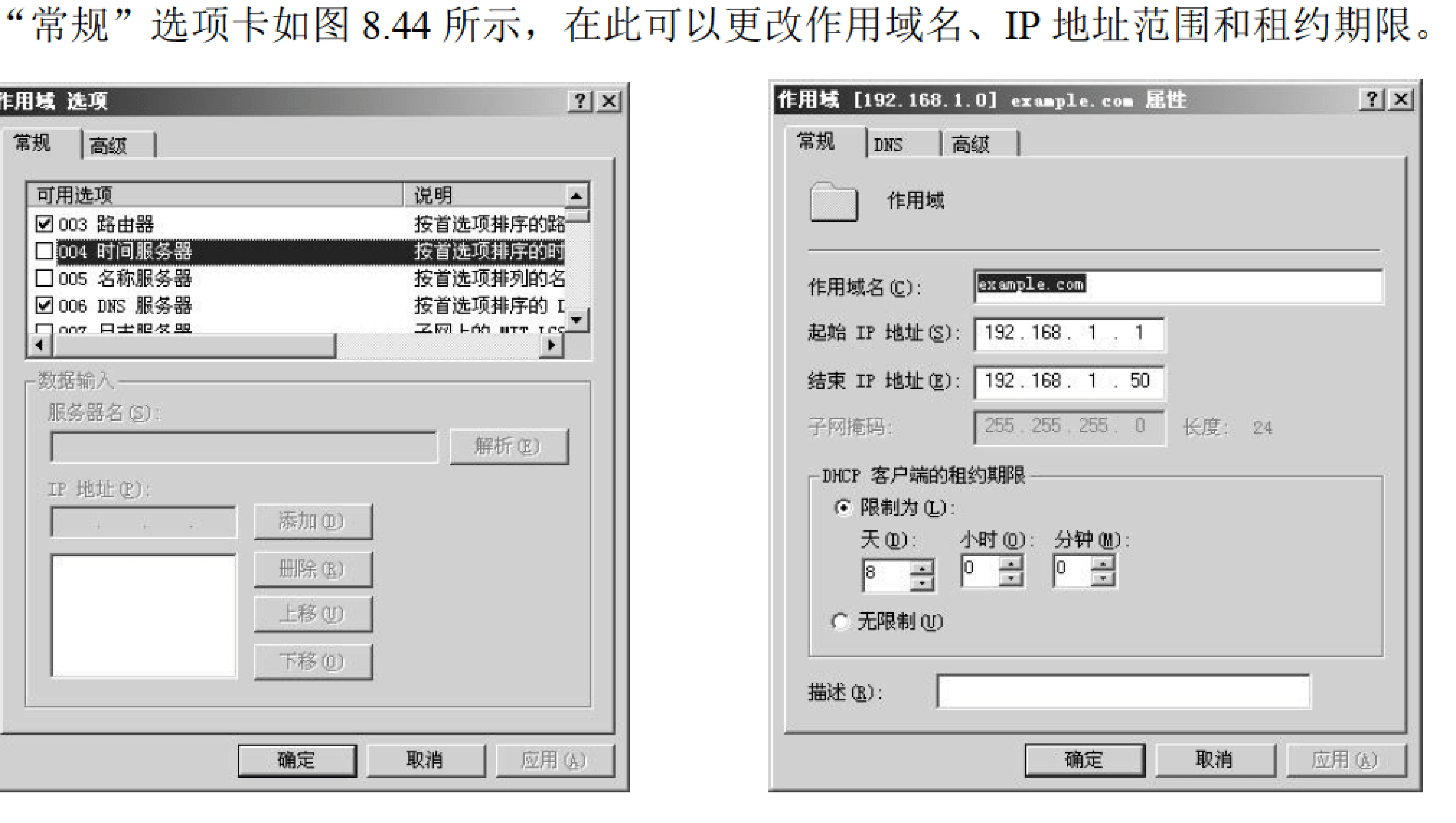


图 8.44　“常规”选项卡



DNS 选项卡可以设置 DHCP 服务器是否启用 DNS 动态更新。启用 DNS 动态更新的好处是当客户端的 IP 地址发生变化后，DHCP 服务器将会发送信息更新 DNS 服务器中该主机的主机和指针记录，以确保信息的一致性。

“高级”选项卡可以指定 DHCP 服务器为哪种类型的客户端动态分配 IP 地址，其中 BOOTP 一般为无盘工作站客户端，若网内没有无盘工作站，选择“仅 DHCP”选项即可。

当安装 DHCP 服务器的计算机同时也是域控制器时，在使用 DHCP 服务器前需对其进行授权，这是因为当错误配置或未授权的 DHCP 服务器被引入网络时，可能会引发问题。例如，如果启动了未授权的 DHCP 服务器，它可能会为客户端租用不正确的 IP 地址或者否认尝试续订当前地址租约的 DHCP 客户端。这两种配置中的任何一个都可能导致启用 DHCP 的客户端产生更多的问题。例如，从未授权的服务器获取配置租约的客户端将找不到有效的域控制器，从而导致客户端无法成功登录到网络。为了避免这些问题，在客户端之前运行 Windows Server 2008 R2 上的 DHCP 服务器服务时，需要验证是否已在 Active Directory 中对它们进行了授权。这样就避免了由于运行带有不正确配置的 DHCP 服务器或者在错误的网络上运行配置正确的服务器而导致的大多数意外破坏。DHCP 服务器一旦在授权列表中发现其 IP 地址，便进行初始化并开始为客户端提供 DHCP 服务。如果在授权列表中未发现自己的地址，则不进行初始化并停止提供 DHCP 服务。

授权的某台 DHCP 服务器的操作方法如下：依次选择“开始”→“管理工具”→DHCP 命令，打开 DHCP 管理控制台。右键单击要授权的服务器名，在弹出的快捷菜单中选择“授权”命令。授权过程需要一段时间，期间用户可以按 F5 键查看状态，检查是否完成授权。

要解除某台已授权服务器的授权，方法与授权过程相同，只是在弹出的快捷菜单中选择“撤销授权”命令即可。

8.2.4　Linux 应用服务器的配置

8.2.4.1　Apache 服务器的配置

1. 主站点的配置

Apache 是使用排名世界第一的 Web 服务器软件。它可以运行在几乎所有广泛使用的计算机平台上。

Apache 源于 NCSAhttpd 服务器，经过多次修改，已成为世界上最流行的 Web 服务器软件之一。Apache 取自 a patchy server 的读音，意思是充满补丁的服务器，因为它是自由软件，所以不断有人来为它开发新的功能、新的特性，修改原来的缺陷。Apache 的特点是简单、速度快、性能稳定，并可作为代理服务器来使用。

Apache 的配置由 httpd.conf 文件配置，因此下面的配置指令都是在 httpd.conf 文件中进行修改。

1) 基本配置

ServerRoot“/mnt/software/apache2”# apache 表示软件安装的位置。其他指定的目录如果没有指定绝对路径，则目录是相对于该目录。“#”后的内容表示对语句的解释。

```
PidFile logs/httpd.pid #第一个 httpd 进程(所有其他进程的父进程)的进程号文件位置
Listen 80 #服务器监听的端口号
```

```
ServerName www.clusting.com:80 #主站点名称(网站的主机名)
ServerAdmin admin@clusting.com #管理员的邮件地址
DocumentRoot "/mnt/web/clusting" #主站点的网页存储位置
```

以下是对主站点的目录进行访问控制。

```
<Directory "/mnt/web/clusting">
Options FollowSymLinks
AllowOverride None
Order allow,deny
Allow from all
</Directory>
```

在上面这段目录属性配置中，主要有以下选项。

(1) Options：配置特定目录使用的相关特性，常用的值和基本含义如下。

- ExecCGI：在该目录下允许执行 CGI 脚本。
- FollowSymLinks：在该目录下允许文件系统使用符号连接。
- Indexes：当用户访问该目录时，如果用户找不到 DirectoryIndex 指定的主页文件(如 index.html)，则返回该目录下的文件列表给用户。
- SymLinksIfOwnerMatch：当使用符号连接时，只有当符号连接的文件拥有者与实际文件的拥有者相同时才可以访问。

(2) AllowOverride：允许可存在于.htaccess 文件中的指令类型(.htaccess 文件名是可以改变的，其文件名由 AccessFileName 指令决定)。

- None：当 AllowOverride 被设置为 None 时，不搜索该目录下的.htaccess 文件(可以减小服务器开销)。
- All：当 AllowOverride 被设置为 All 时，在.htaccess 文件中可以使用所有的指令。

(3) Order：控制在访问时 allow 和 deny 两个访问规则哪个优先。

- allow：允许访问的主机列表(可用域名或子网，例如 Allow from 192.168.0.0/16)。
- deny：拒绝访问的主机列表。

以下是对首页文件的格式进行设置。

```
DirectoryIndex index.html index.htm index.php #主页文件的设置(将主页文件设置为
index.html,index.htm 和 index.php)
```

2) 服务器的优化

Apache 主要的优势就是对多处理器的支持更好，在编译时通过使用--with-mpm 选项来决定 Apache2 的工作模式。如果知道当前的 Apache2 使用什么工作机制，可以通过 httpd -l 命令列出 Apache 的所有模块，就可以知道其工作方式了。

(1) prefork：如果 httpd -l 列出 prefork.c，则需要对下面的段进行配置。

```
<IfModule prefork.c>
StartServers 5 #启动 Apache 时启动的 httpd 进程个数
MinSpareServers 5 #服务器保持的最小空闲进程数
MaxSpareServers 10 #服务器保持的最大空闲进程数
MaxClients 150 #最大并发连接数
```

```
MaxRequestsPerChild 1000 #每个子进程被请求服务多少次后被 kill 掉。0 表示不限制，推荐设置为 1000
</IfModule>
```

在该工作模式下，服务器启动后启动 5 个 httpd 进程(连同父进程共 6 个，通过 ps -ax|grep httpd 命令可以看到)。当有用户连接时，Apache 会使用一个空闲进程为该连接服务，同时父进程会 fork 一个子进程，直到内存中的空闲进程达到 MaxSpareServers 为止。该模式是为了兼容一些旧版本的程序，是默认编译时的选项。

(2)　worker：如果 httpd -l 列出 worker.c，则需要对下面的段进行配置。

```
<IfModule worker.c>
StartServers 2 #启动 Apache 时启动的 httpd 进程个数
MaxClients 150 #最大并发连接数
MinSpareThreads 25 #服务器保持的最小空闲线程数
MaxSpareThreads 75 #服务器保持的最大空闲线程数
ThreadsPerChild 25 #每个子进程产生的线程数
MaxRequestsPerChild 0 #每个子进程被请求服务多少次后被 kill 掉。0 表示不限制，推荐设置为 1000
</IfModule>
```

该模式是由线程来监听客户的连接。当有新客户连接时，由其中的一个空闲线程接受连接。服务器在启动时启动两个进程，每个进程产生的线程数是固定的(由 ThreadsPerChild 决定)，因此启动时有 50 个线程。当 50 个线程不够用时，服务器自动 fork 一个进程，再产生 25 个线程。

(3)　perchild：如果 httpd -l 列出 perchild.c，则需要对下面的段进行配置。

```
<IfModule perchild.c>
NumServers 5 #服务器启动时启动的子进程数
StartThreads 5 #每个子进程启动时启动的线程数
MinSpareThreads 5 #内存中的最小空闲线程数
MaxSpareThreads 10 #最大空闲线程数
MaxThreadsPerChild 2000 #每个线程最多被请求多少次后退出。0 表示不受限制
MaxRequestsPerChild 10000 #每个子进程服务多少次后被重新 fork。0 表示不受限制
</IfModule>
```

在该模式下，子进程的数量是固定的，线程数不受限制。当客户端连接到服务器时，由空闲的线程提供服务。如果空闲线程数不够，子进程会自动产生线程来为新的连接服务。该模式用于多站点服务器。

3) HTTP 返回头信息配置

(1)　ServerTokens Prod #该参数设置 http 头部返回的 Apache 版本信息，可用的值和含义如下。

- Prod：仅软件名称，例如 Apache。
- Major：包括主版本号，例如 Apache/2。
- Minor：包括次版本号，例如 Apache/2.0。
- Min：仅 Apache 的完整版本号，例如 Apache/2.0.54。

- OS：包括操作系统类型，例如 Apache/2.0.54(Unix)。
- Full：包括 Apache 支持的模块及模块版本号，例如 Apache/2.0.54 (Unix) mod_ssl/2.0.54 OpenSSL/0.9.7g。

(2) ServerSignature Off#在页面产生错误时是否出现服务器版本信息，推荐设置为 Off。

4) 持久性连接设置

KeepAlive On #开启持久性连接功能，即当客户端连接到服务器，下载完数据后仍然保持连接状态。

```
MaxKeepAliveRequests 100 #一个连接服务的最多请求次数
KeepAliveTimeout 30 #持续连接多长时间，若该连接没有再请求数据，则断开该连接。默认为
15 秒
```

2. 别名设置

对于不在 DocumentRoot 指定目录内的页面，既可以使用符号连接，也可以使用别名连接。别名的设置如下。

```
Alias /download/ "/var/www/download/" #访问时可以输入:http://www.custing.
com/download/
<Directory "/var/www/download"> #对该目录进行访问控制设置
Options Indexes MultiViews
AllowOverride AuthConfig
Order allow,deny
Allow from all
</Directory>
```

3. CGI 设置

通过 http://www.clusting.com/cgi-bin/ 可以访问 ScriptAlias /cgi-bin/ "/mnt/software/apache2/cgi-bin/"。但是，该目录下的 CGI 脚本文件要加可执行权限，其设置如下。

```
<Directory "/usr/local/apache2/cgi-bin"> #设置目录属性
AllowOverride None
Options None
Order allow,deny
Allow from all
</Directory>
```

4. 日志的设置

1) 错误日志的设置

```
ErrorLog logs/error_log #日志的保存位置
LogLevel warn #日志的级别
```

显示的格式如下。

```
[Mon Oct 10 15:54:29 2005] [error] [client 192.168.10.22] access to /download/
failed, reason: user admin not allowed access
```

2) 访问日志设置

日志的默认格式有以下几种。



```
LogFormat "%h %l %u %t "%r" %>s %b "%{Referer}i" "%{User-Agent}i" " combined
LogFormat "%h %l %u %t"%r" %>s %b" common #common 为日志格式名称
LogFormat "%{Referer}i -> %U" referer
LogFormat "%{User-agent}i" agent
CustomLog logs/access_log common
```

格式中各个参数的意义如下。

- %h：客户端的 IP 地址或主机名。
- %l：这是由客户端 identd 判断的 RFC 1413 身份，输出中的符号“-”表示此处信息无效。
- %u：由 HTTP 认证系统得到的访问该网页的客户名。有认证时才有效，输出中的符号“-”表示此处信息无效。
- %t：服务器完成对请求的处理所用的时间。
- “%r”：引号中是客户发出的包含了许多有用信息的请求内容。
- %>s：这是服务器返回给客户端的状态码。
- %b：这项是返回给客户端的不包括响应头的字节数。
- “%{Referer}i”：此项指明了该请求是从哪个网页提交过来的。
- “%{User-Agent}i”：此项是客户浏览器提供的浏览器识别信息。

5. 用户认证的配置

1) httpd.conf 文件的配置

假定对目录/var/www/download 下的文件需要做到 Apache 用户认证，则在 httpd.conf 中加入下面的代码。

```
AccessFileName .htaccess
...
Alias /download/ "/var/www/download/"
<Directory "/var/www/download">
Options Indexes
AllowOverride AuthConfig
</Directory>
```

2) 建立一个口令文件

Apache 自带的 htpasswd 提供了建立和更新存储用户名、密码口令文件的功能，其配置语句如下。

```
/usr/local/apache2/bin/htpasswd -c /var/httpuser/passwords bearzhang
onfigure the server to request a password and tell the server which users
are allowed access.
vi /var/www/download/.htaccess:
AuthType Basic
AuthName "Restricted Files"
AuthUserFile /var/httpuser/passwords
Require user bearzhang
#Require valid-user #all valid user
```

6. 用户认证的虚拟主机的配置

1) 基于 IP 地址的虚拟主机配置

基于 IP 地址的虚拟主机配置代码如下。

```
Listen 80
<VirtualHost 172.20.30.40>
DocumentRoot /www/example1
ServerName www.example1.com
</VirtualHost>
<VirtualHost 172.20.30.50>
DocumentRoot /www/example2
ServerName www.example2.org
</VirtualHost>
```

2) 基于 IP 和多端口的虚拟主机配置

基于 IP 和多端口的虚拟主机配置代码如下。

```
Listen 172.20.30.40:80
Listen 172.20.30.40:8080
Listen 172.20.30.50:80
Listen 172.20.30.50:8080

<VirtualHost 172.20.30.40:80>
DocumentRoot /www/example1-80
ServerName www.example1.com
</VirtualHost>

<VirtualHost 172.20.30.40:8080>
DocumentRoot /www/example1-8080
ServerName www.example1.com
</VirtualHost>

<VirtualHost 172.20.30.50:80>
DocumentRoot /www/example2-80
ServerName www.example1.org
</VirtualHost>

<VirtualHost 172.20.30.50:8080>
DocumentRoot /www/example2-8080
ServerName www.example2.org
</VirtualHost>
```

3) 单个 IP 地址的服务器上基于域名的虚拟主机配置

单个 IP 地址的服务器上基于域名的虚拟主机配置代码如下。

```
# Ensure that Apache listens on port 80
Listen 80

# Listen for virtual host requests on all IP addresses
NameVirtualHost *:80
```





```
<VirtualHost *:80>
DocumentRoot /www/example1
ServerName www.example1.com
ServerAlias example1.com. *.example1.com
# Other directives here
</VirtualHost>

<VirtualHost *:80>
DocumentRoot /www/example2
ServerName www.example2.org
# Other directives here
</VirtualHost>
```

4) 在多个 IP 地址的服务器上配置基于域名的虚拟主机

在多个 IP 地址的服务器上配置基于域名的虚拟主机的代码如下。

```
Listen 80

# This is the "main"server running on 172.20.30.40
ServerName server.domain.com
DocumentRoot /www/mainserver

# This is the other address
NameVirtualHost 172.20.30.50

<VirtualHost 172.20.30.50>
DocumentRoot /www/example1
ServerName www.example1.com
# Other directives here ...
</VirtualHost>

<VirtualHost 172.20.30.50>
DocumentRoot /www/example2
ServerName www.example2.org
# Other directives here ...
</VirtualHost>
```

5) 在不同的端口上运行不同的站点(基于多端口的服务器上配置基于域名的虚拟主机)

实现在不同的端口上运行不同站点的配置代码如下。

```
Listen 80
Listen 8080

NameVirtualHost 172.20.30.40:80
NameVirtualHost 172.20.30.40:8080

<VirtualHost 172.20.30.40:80>
ServerName www.example1.com
DocumentRoot /www/domain-80
</VirtualHost>
```

```
<VirtualHost 172.20.30.40:8080>
ServerName www.example1.com
DocumentRoot /www/domain-8080
</VirtualHost>

<VirtualHost 172.20.30.40:80>
ServerName www.example2.org
DocumentRoot /www/otherdomain-80
</VirtualHost>

<VirtualHost 172.20.30.40:8080>
ServerName www.example2.org
DocumentRoot /www/otherdomain-8080
</VirtualHost>
```

6) 基于域名和基于 IP 的混合虚拟主机的配置

基于域名和基于 IP 的混合虚拟主机的配置代码如下。

```
Listen 80
NameVirtualHost 172.20.30.40

<VirtualHost 172.20.30.40>
DocumentRoot /www/example1
ServerName www.example1.com
</VirtualHost>

<VirtualHost 172.20.30.40>
DocumentRoot /www/example2
ServerName www.example2.org
</VirtualHost>

<VirtualHost 172.20.30.40>
DocumentRoot /www/example3
ServerName www.example3.net
</VirtualHost>
```

8.2.4.2 DNS 服务器的配置

1. 配置转换程序

使用 DNS 的第一步是在用户的计算机上配置转换程序，即让机器能够从 DNS 服务器中获取域名解析/反解析服务。转换程序不是一个单独而明确的处理进程，而是网络进程调用的一个标准 C 程序库。如果本地系统不运行 named，就必须配置本地转换程序。

1) 转换程序的控制文件/etc/host.conf

/etc/host.conf 文件是用来控制本地转换程序文件的设置。该文件告诉转换程序使用哪些服务、按照什么顺序进行。该文件的字段可以用空格或制表符分隔。字符“#”表示注释行。/etc/host.conf 文件的配置选项如下。

- order：指定按照哪种顺序来尝试不同的名字解析机制，按列出的顺序来进行指定的解析服务，支持下面的名字解析机制。

- ◆ hosts：试图通过查找本地/etc/hosts 文件来解析名字。
- ◆ bind：使用 DNS 域名服务器来解析名字。
- ◆ nis：使用网络信息服务(NIS)协议来解析主机名字。

- multi：以 off 和 on 为参数。与 host 查询一起使用，用来确定一台主机是否在/etc/hosts 文件中指定了多个 IP 地址。
- nospoof：如果用逆向解析找出与指定的地址匹配的主机名，就可以对返回的地址进行解析以确认它确实与查询的地址相配。为了防止“骗取”IP 地址，可通过指定 nospoof on 来允许逆向解析功能。
- alert：以 off 和 on 为参数。如果打开，任何试图骗取 IP 地址的行为都通过 syslog 工具被记录下来。
- trim：以域名为参数。在/etc/hosts 中查找名字前，trim 删除这个域名，只把基本主机名放在/etc/host.conf 中而不指定域名。

下面这个例子是主机 vlager 上的/etc/host.conf 文件。

```
# /etc/host.conf
# We have named running, but no NIS (yet)
order bind hosts
# Allow multiple address
multi on
# Guard against spoof attempts
nospoof on
# Trim local domain (not really necessary).
trim vbrew.com.
```

这个例子给出了域 vbrew.com 的通用解析程序配置。该解析程序首先使用 DNS 解析，然后使用/etc/hosts 文件查找主机名。在解析查找中指定本地/etc/hosts 文件是一个好主意。如果由于某种原因不能使用域名服务器了，我们还可以使用主机文件中列出的那些主机名。该机器上允许使用多个 IP 地址，主机通过重新解析主机名字(从 IP 地址逆向查找返回的主机名字)来检查 IP 欺骗。

2) 转换程序的配置文件/etc/resolv.conf

当配置转换程序使用 BIND 域名服务查询主机时，我们必须告诉转换程序使用哪一个域名服务器。用来完成这项任务的工具就是/etc/resolv.conf 文件。该文件控制转换程序采用 DNS 解析主机名时使用的方式，可以明确地定义系统的配置，允许我们命名由于默认服务器不响应而使用的备份服务器。因此，尽管会增加系统负荷，但在某些场合使用 resolv.conf 是很受欢迎的。

/etc/resolv.conf 是一个简单而易读的文件。在/etc/resov.conf 中使用的命令，具有系统专用的形式，但一般都支持 nameserver 和 domain 两项命令。

nameserver 项利用 IP 地址去识别，让转换程序去识别查询域信息的那些服务器。我们可以通过多次使用 nameserver 选项，使用多达 3 个域名服务器。这些域名服务器是按照它们在文件中的顺序进行查询的，如果没有接收到任何一个服务器的响应，就去试表中的下一个服务器，直到所有服务器试完为止(如果在/etc/resolv.conf 文件中设置了 3 个以上的域名服务器，那么，即使前 3 个服务器都没有响应查询请求，Linux 也不会去请求后面的服务器)。我们应该将最可靠的域名服务器列在最前面，以便在查询时不会超时。如果 resolv.conf 文

件中不包含 nameserver 项，或者不存在 resolv.conf 文件，就将所有域名服务器查询发送给本地主机。然而，如果有一个 resolv.conf 文件，它包含 nameserver 项，除非有一项指向本地主机，否则就不查询本地主机。在配置唯转换程序的主机中，resolv.conf 文件包含 nameserver 项，但没有一个项指向本地主机。

domain 项用来定义默认域名(主机的本地域名)。转换程序会将默认域名挂接在任何不含点的主机名后面。例如，转换程序接收到主机名 vale(它不含点)，就将其默认域名挂接在 vale 后面，对它进行查询。如果 domain 域中的 name 值是 vbrew.com，那么转换程序就将查询 vale.vbrew.com。如果没有找出它，则转换程序就试图通过 getdomainname()系统调用函数来获得本地域名。

如果对上面的解释不理解，可以看看下面这个例子，这是 Virtual Brewery 中的 resolv.conf 文件。

```
# /etc/resolv.conf
# Our domain
domain vbrew.com
#
# We use vlager as central nameserver:
nameserver 191.72.1.1
```

在该例中，通过 domain 项指定默认域名，并列出一个用于解析主机名的域名服务器。在这个例子中没有指定查询顺序(使用 search 选项)，因此如果要查询一台机器的地址(如 vale)，解析器首先试图查找 vale，如果没找到，则查找 vale.vbrew.com，然后再查找 vbrew.com。

2. 唯转换程序配置

配置唯转换程序是非常简单的，下面是一个唯转换程序的/etc/resolv.conf 文件的例子。

```
# /etc/resolv.conf
# Our domain
domain vbrew.com
#
# We use vlager as central nameserver:
nameserver 191.72.1.1
# next try vale
nameserver 191.72.1.3
```

该配置文件告诉转换程序将所有的查询发送给主域名服务器 vlager，如果失败，就试 vale。这些查询是永远不能在本地转换的。这个简单的 resolv.conf 文件就可以满足唯转换程序配置的全部要求。

3. 设置域名服务器

在 Linux 上的域名服务是由 named 守护进程来执行的，named 最早是为 BSD 向客户机提供域名服务而开发的。named 守护进程通常在系统启动时开始工作，并一直工作到系统关闭。该进程从被称作/etc/named.boot 的配置文件中获取有关信息并将主机名映射为 IP 地址的各种文件。

为了运行 named，只要在命令行中输入# /etc/rc.d/init.d/named start，named 就会开始运行，读取 named.boot 文件及其定义的任意区文件，并将它的进程 ID 以 ASCII 码的形式写入/var/run/named.pid 中，下载任何来自主服务器的区文件，如果有必要的话在端口 53 等待 DNS 请求。

下面介绍与 DNS 有关的几个配置文件以及它们的功能。

- named.conf：设置一般的 named 参数，指向该服务器使用的域数据库信息的源，这类源可以是本地磁盘文件或远程服务器。
- named.ca：指向根域名服务器。
- named.local：用于在本地转换回送地址。
- named.hosts：将主机名映射为 IP 地址。
- named.rev：用于反向域的、将 IP 地址映射到主机名的区文件。

理解不同配置的最佳方法是讨论各种 named.conf 的示例文件。

1) 唯高速缓存服务器

配置唯高速缓存域名服务器是很简单的，必须有 named.conf 和 named.ca 文件，通常也要用到 named.local 文件。下面是用于唯高速缓存服务器的 named.conf 文件的例子，其中以“//”开头的是注释。

```
// generated by named-bootconf.pl
options {
directory "/var/named";
/*
* If there is a firewall between you and nameservers you want
* to talk to, you might need to uncomment the query-source
* directive below. Previous versions of BIND always asked
* questions using port 53, but BIND 8.1 uses an unprivileged
* port by default.
*/
// query-source address * port 53;
};
//
// a caching only nameserver config
//
zone "." {
type hint;
file "named.ca";
};
zone "0.0.127.in-addr.arpa" {
type master;
file "named.local";
};
```

directory 这一行告诉 named 到哪里去找寻文件。所有其后命名的文件都是相对于此目录的。该文件告诉 named 去维持一个域名服务器响应的高速缓存，并利用 named.ca 文件的内容去初始化该高速缓存。该高速缓存初始化文件的名字可以是任何名字，但一般使用 /var/named/named.ca。并不是在该文件中使用一个 hint 语句就能使它成为唯高速缓存配置，而是因为没有 master 和 slave 语句才使它成为一个唯高速缓存配置文件。

但是，在这个例子中有一个 master 语句。事实上，几乎在每一个唯高速缓存的配置文件中都有这一语句，它将本地服务器定义为它自己的回送域的主服务器，并假定该域的信息存储在 named.local 文件中。这个回送域是一个 in-addr.arpa 域(in-addr.arpa 域用于指定逆向解析，或 IP 地址到 DNS 名字解析)，它将地址 127.0.0.1 映射为名字 localhost。转换自己的回送地址对于大多数人都是有意义的，因此许多 named.conf 文件都包含这一项。

在大多数唯高速缓存服务器的配置文件中，像 directory、master 和 hint 语句都是唯一使



用的语句，但也可以增加其他的语句，比如 forwarders 和 slave 等语句都可以使用。

2) 主服务器和辅助服务器的配置

我们虚构的 vbrew.com 是举例说明主服务器和辅助服务器的基础，下面是将 vlager 定义为 vbrew.com 域主服务器的 named.conf 文件。

```
// generated by named-bootconf.pl
options {
directory "/var/named";
/*
* If there is a firewall between you and nameservers you want
* to talk to, you might need to uncomment the query-source
* directive below. Previous versions of BIND always asked
* questions using port 53, but BIND 8.1 uses an unprivileged
* port by default.
*/
// query-source address * port 53;
};
//
// a caching only nameserver config
//
zone "." {
type hint;
file "named.ca";
};
zone "vbrew.com"{
type master;
file "named.hosts";
};
zone "0.0.127.in-addr.arpa" {
type master;
file "named.local";
};
zone "72.191.in-addr.arpa"{
type master;
file "named.rev";
};
```

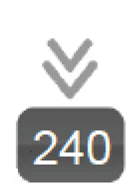
上例中第一个 master 告诉我们这是 vbrew.com 域的主服务器。该域的数据是从 named.hosts 文件中加载的。在这个例子中，我们可以将文件名 named.hosts 作为区文件名，也可以使用更有说明性的文字。例如 vbrew.com 区文件的名字使用 vbrew.com.hosts 则较好。

第三个 master 语句指向能将 IP 地址 191.72.0.0 映射为主机名的文件。它假定本地服务器是反向域 72.191.in-addr.arpa 的主服务器，该域的数据从文件 named.rev 中加载。

对于上例配置中的 hint 语句和第二个用于回送域的 primary 语句，我们在前面唯高速缓存配置中已经讨论过。在这些配置中，它们的作用是相同的，而且几乎在任何配置中都要使用它们。

辅助服务器的配置与主服务器的配置不同，它使用 slave 语句代替 master 语句。slave 语句指向用作域信息源的远程服务器，以替代本地磁盘文件。下面的 named.conf 文件可以将 vale 配置成 vbrew.com 域的辅助服务器。

```
// generated by named-bootconf.pl
options {
directory "/var/named";
/*
```



```
* If there is a firewall between you and nameservers you want
* to talk to, you might need to uncomment the query-source
* directive below. Previous versions of BIND always asked
* questions using port 53, but BIND 8.1 uses an unprivileged
* port by default.
*/
// query-source address * port 53;
};
//
// a caching only nameserver config
//
zone "." {
type hint;
file "named.ca";
};
zone "0.0.127.in-addr.arpa"{
type master;
file "named.local";
};
zone "vbrew.com"{
type slave;
file "named.hosts";
masters { 191.72.1.3; };
};
zone "72.191.in-addr.arpa"{
type slave;
file "named.rev";
masters {191.72.1.3;};
};
cache . named.ca
secondary vbrew.com 191.72.1.3 named.hosts
secondary 72.191.in-addr.arpa 191.72.1.3 named.rev
primary 0.0.127.in-addr.arpa named.local
```

第一个 slave 语句是使这个服务器成为 vbrew.com 的辅助服务器。它告诉 named 从 IP 地址为 191.72.1.3 的服务器中下载 vbrew.com 的信息，并将其数据保存在/var/named/named.hosts 文件中。如果该文件不存在，named 就创造一个，并从远程服务器中取得区数据，然后将这些数据写入新创建的文件中。如果存在该文件，named 就要检查远程服务器，以了解远程服务器的数据是否不同于该文件中的数据，如果数据有变化，它就下载更新后的数据，用新数据覆盖该文件的内容；如果数据没有变化，named 就加载磁盘文件的内容，而不必做麻烦的区转移工作。

将一个数据库复制到本地磁盘文件中后，就不必在每次引导主机时都要转移区文件；只有当修改数据时，才进行这种区文件的转移工作。

配置文件中的下一行表示该本地服务器也是反向域 72.191.in-addr.arpa 的一个辅助服务器，而且该域的数据也从 191.72.1.3 中下载。反向域的数据存储在 named.rev 中。

DNS 数据库文件和资源记录配置 named 所需的所有文件(named.hosts、named.rev、named.local 和 named.ca)中的信息都是以资源记录的形式存在的。每个资源记录都有一个类型，这个类型说明记录的功能。这些记录都是标准资源记录，称为 RR(Resource Records)。

8.2.4.3　DHCP 服务器的配置

DHCP 的配置文件是/etc/dhcpd.conf，不过默认情况下这个文件不存在，需要使用它的



模板建立一个配置文件。模板的位置在/user/share/doc/dhcp-3.0p11/dhcpd.conf.sample 中。

模板配置文件的内容如下。

```
ddns-update-style interim;
#配置使用过渡性 DHCP-DNS 互动更新模式
ignore client-updates;
#忽略客户端更新
subnet 192.168.0.0 netmask 255.255.255.0 {
#设置子网声明
# --- default gateway
option routers 192.168.0.1;
#设置默认网关为 192.168.0.1

option subnet-mask 255.255.255.0;
#设置客户端的子网掩码
option nis-domain "domain.org";
#为客户设置 NIS 域
option domain-name "domain.org";
#为客户设置域名
option domain-name-servers 192.168.1.1;
#为客户设置域名服务器
option time-offset -18000; # Eastern Standard Time
#设置偏移时间
option ntp-servers 192.168.1.1;
#设置 NTP 服务器
option netbios-name-servers 192.168.1.1;
#设置 WINS 服务器
# --- Selects point-to-point node (default is hybrid). Don't change this unless
# -- you understand Netbios very well
option netbios-node-type 2;
#设置 netbios 节点类型
range dynamic-bootp 192.168.0.128 192.168.0.255;
#设置动态的地址池
default-lease-time 21600;
#设置默认的地址租期
max-lease-time 43200;
#设置客户端最长的地址租期

# we want the nameserver to appear at a fixed address
//设置主机声明
host ns {
next-server marvin.redhat.com;
//设置定义服务器从引导文件中装入的主机名，用于无盘站
hardware ethernet 12:34:56:78:AB:CD;
//指定 DHCP 客户的 MAC 地址
fixed-address 207.175.42.254;
//给指定的 MAC 地址分配 IP
}
}
```

8.2.4.4 Samba 服务器的配置

Samba 能够使 Windows 用户通过网上邻居等熟悉的方式直接访问 Linux 上的资源，也

能使 Linux 利用 SMB 客户端程序访问 Windows 的共享资源。

提示：服务信息块(Server Message Block，SMB)是局域网上的共享文件夹/打印机的一种协议。

下面以一个具体的例子对 Samba 服务器的配置进行说明。

```
[global]
   workgroup = WORKGROUP
   server string = Samba Server
   printcap name = /etc/printcap
   load printers = yes
cups options = raw
log file = /var/log/samba/%m.log
   max log size = 50
   security = user
   socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
   dns proxy = no
   idmap uid = 16777216-33554431
   idmap gid = 16777216-33554431
   template shell = /bin/false
   winbind use default domain = no
[homes]
   comment = Home Directories
   browseable = no
   writable = yes
[printers]
   comment = All Printers
   path = /var/spool/samba
   browseable = no
   guest ok = no
   writable = no
   printable = yes
```

从上面的程序中可以看到 Samba 的配置文件分为 3 节。

- [global]：这个小节主要包含全局参数。
- [homes]：这个小节用于共享存储在\home 中的 Linux 用户目录。
- [printers]：这个小节用于共享本地 Linux 打印机文件/etc/printcap 中列出的所有打印机。

1. [global] 全局参数配置

[global] 全局参数配置命令如下。

```
workgroup = WORKGROUP
netbios = dolinux.cn
server string = NetSeek's Samba Server(%h Samba Server)
hosts allow = netseek,cnseek.org,192.168.0.*EXPECT 192.168.0.5
//允许主机名为 netseek 的客户端访问，允许域为 cnseek.org 的域访问，允许 192.168.0.*
//所有的主机访问，除了 192.168.0.5 之外
printcap name = /etc/printcap  //Samba 启动时，将会自动加载打印机配置文件，建议
//默认即可
load printers = yes            //允许自动加载浏览列表，默认即可
log file = /var/log/samba/%m.log  //samba 相关的日志文件
security = user   //使用的安全等级，默认值为 user
password level = 8
username level = 8  //用户名和密码长度限制
```



```
encrypt passwords = yes  //使用口令加密
smb passwd file = /etc/samba/smbpasswd //Smaba 账号存放文件，注意务必采用加密形
        //式，否则要改 win 注册表，因为 win 也采用了加密方式
username map = /etc/samba/smbusers //用户映射，将不同的用户映射成为一个用户
```

安全等级分为以下 5 类。

- share。当客户端连接到该等级的 Samba 服务器上时，不需要输入账号和密码，就可以访问 Samba 服务器上的共享资源，但安全性无法保证。
- user。用户需要输入有效的密码，通过验证后才能使用服务器的共享。
- server。与 user 等级相同，也需要输入有效的账号和密码，但还需要指定口令服务器。其配置命令如下。

  ```
  password server =  <NT-Server-Name>
  eg: security = server
  password server= SMB2
  smb passwd file =/etc/samba/smbpasswd_smb2
  ```

- domain 安全等级。domain 安全等级表示指定 Windows 域控制服务器来验证用户账户及密码。Samba 服务器加入到 Windows NT 域中后，Samba 服务器不再负责账号和密码的验证，而是统一由域控制器负责，此时需要使用访问安全等级，同时也必须指定口令服务器。
- ads 安全等级。Samba 服务器加入到 Windows 活动目录后，需要使用访问安全等级，同时也需要指定口令服务器。

2. [homes] 设置共享目录

[homes]设置共享目录的配置命令如下。

```
[homes]
 comment = Home Directories//目录文字说明
browseable = no            //是否允许用户浏览 homes 主目录，建议使用默认值不允许
writable = yes             //是否允许写入个人主目录
comment = 文字说明内容         //文字说明
browseable = no //表示禁止浏览，也就是本目录只有有权使用的用户可以看到
writable = yes //允许有权限的用户写入
valid users = netseek,lin,@share //只允许 netseek、lin、用户 share 组的访问
```

设置一个共享目录的命令如下。

```
[shares]
 comment = NetSeek's share Directory
read list = netseek
 write list = @share
 path = /home/share
```

说明： netseek 的用户可以读，share 组的用户可以读写，所有验证通过的用户对这个目录可读可写。

3. [printers] 共享打印

[printers] 共享打印的配置命令如下。

```
   comment = All Printers
   path = /var/spool/samba
   browseable = no
```



```
   //如果允许 guest 打印，只需在末尾加入 public = yes 即可
# Set public = yes to allow user 'guest account' to print
   guest ok = no
   writable = no
   printable = yes
```

4. 用户创建

(1) 系统用户映射给 Samba，其配置命令如下。

```
#cat /etc/passwd | /usr/bin/mksmbpasswd.sh > /etc/samba/smbpasswd
```

(2) 为用户添加 SMB 口令，其配置命令如下。

```
#smbpasswd netseek
New SMB password:*******
Retype new SMB password:*******
```

5. 服务启动

服务启动的命令如下。

```
/etc/rc.d/init.d/smb start
/etc/rc.d/init.d/smb restart
#chkconfig smb on
#chkconfig --list smb
```

8.3 真题详解

8.3.1 综合知识试题

试题 1 (2017 年下半年试题 31)

在 Linux 中，要复制整个目录，应使用<u>(31)</u>命令。

(31) A. cat-a　　B. mv-a　　C. cp-a　　D. rm-a

参考答案：(31)C。

要点解析：在 Linux 中 cp 为复制命令。

试题 2 (2017 年下半年试题 32)

在 Linux 中，<u>(32)</u>是默认安装 DHCP 服务器的配置文件。

(32) A. /etc/dhcpd.conf　　B. /etc/dhcp.conf
　　C. /var/dhcpd.conf　　D. /var/dhcp.conf

参考答案：(32)A。

要点解析：考查 Linux 基本配置文件的名字和路径。默认 DHCP 服务器的配置文件为/etc/dhcpd.conf。

试题 3 (2017 年下半年试题 33)

<u>(33)</u>是 Linux 中 Samba 的功能。

(33) A. 提供文件和打印机共享服务　　B. 提供 FTP 服务

C. 提供用户的认证服务　　D. 提供 IP 地址分配服务

参考答案：(33)A。

要点解析：Samba 在 Linux 中是一项提供文件和打印机共享的基本服务。

试题 4 (2017 年下半年试题 34)

在进行域名解析的过程中，若主域名服务器故障，由转发域名服务器传回解析结果，下列说法中正确的是 (34) 。

(34) A. 辅助域名服务器配置了递归算法
B. 辅助域名服务器配置了迭代算法
C. 转发域名服务器配置了递归算法
D. 转发域名服务器配置了迭代算法

参考答案：(34)C。

要点解析：通常本地 DNS 服务器使用递归形式查询，除此之外，转发域名服务器也使用递归算法。

试题 5 (2017 年下半年试题 35)

在 DNS 资源记录中， (35) 记录类型的功能是实现域名与其别名的关联。

(35) A. MX　　B. NS　　C. CNAME　　D. PTR

参考答案：(35)C。

要点解析：CNAME 实现别名记录，实现同一台服务器可提供多种服务。

试题 6 (2017 年下半年试题 36)

在 Windows 环境下，租约期满后，DHCP 客户端可以向 DHCP 服务器发送一个 (36) 报文来请求重新租用 IP 地址。

(36) A. Dhcpdiscover　　B. Dhcprequest　　C. Dhcprenew　　D. Dhcpsack

参考答案：(36)A。

要点解析：DHCP 典型报文中没有 dhcprenew 这个报文，重新申请 IP 地址还是使用 dhcpdiscover 来实现。

试题 7 (2017 年下半年试题 37)

在运行 Windows Server 2008 R2 的 DNS 服务器上要实现 IP 地址到主机名的映射，应建立 (37) 记录。

(37) A. 指针(PTR)　　B. 主机信息(HINFO)
C. 服务位置(SRV)　　D. 规范名称(CNAME)

参考答案：(37)A。

要点解析：实现 IP 地址到主机名的映射，是一种与域名到 IP 地址相反的映射，使用指针实现。

试题 8 (2017 年下半年试题 43)

在某台 PC 上运行 ipconfig /all 命令后得到如下结果，下列说法中正确的是 (43) 。

Windows IP Configuration

Host Name . . . .:MSZFA2SWBGXX4UT

primary Dns Suffix……:

Node Type . . . . :Hybrid

IP Routing Enabled. . . . . :No

WINS Proxy Enabled…… :No

DNS Suffix Search List. …… :home

Wireless LAN adapter:

Connection-specific DNS Suffix.:home

Description . . . . :Realtek RTL8188EU Network Adapter

Physical Address. . . . . : 30-B4-9E-12-F2-ED

DHCP Enabled. . . . . :Yes

Autoconfiguration Enabled . . . :Yes

Link -local IPv6 Address . .. . :fe80::40bl:7a3a:6cd2:1193%12(peferred)

IPv4Address. . . . .:   192.168.3.12(preferred)

Subnet mask . . . . : 255.255.255.0

Lease Obtained. . . . . :2017-7-15 20:01:59

Lease Expires .. . .: 2017-7-16 20:01:59

Default Gateway . . . . : 192.168.3.1

DHCP.Server . . . . :10.10.20.3

DHCPv6IAID . . . . :222857938

DHCPv6Client DU1D . . . . :00-01-00-01-1F-88-22-5F-74-DO-2B-7B-88-29

DNS Servers . . . . : 8.8.8.8

192.168.3.1

NetBIOS over Tepip . . . . : Enabled

(43) A. IP 地址 192.168.3.12 是该 PC 未续约过的 IP 地址

B. 该 PC 的 IP 地址租期为 12 小时

C. 该 PC 与 DHCP 服务器位于同一个网段

D. 进行 DNS 查询时首先查询服务器 8.8.8.8

参考答案：(43)D。

要点解析：DHCP 服务器默认首选分配客户机曾经使用过的 IP 地址，且租约由 15 日到 16 日为 24 小时，DHCP 服务器指定为客户分配的第一个 DNS 服务器地址为 8.8.8.8。

试题 9 （2017 年下半年试题 61）

在 Windows 用户管理中，使用组策略 A-G-DL-P，其中 A 表示 (61) 。

(61) A. 用户账号　　B. 资源访问权限

C. 域本地组　　D. 通用组

参考答案：(61)A。

要点解析：A 表示用户账号，G 表示全局组，DL 表示域本地组，P 表示资源权限。

试题 10 (2017 年上半年试题 31)

下面关于 Linux 目录的描述中，正确的是___(31)___。

(31) A. Linux 只有一个根目录，用"/root"表示

B. Linux 中有多个根目录，用"/"加相应目录名称表示

C. Linux 中只有一个根目录，用"/"表示

D. Linux 中有多个根目录，用相应目录名称表示

参考答案：(31)C。

要点解析：在 Linux 中，根目录只有一个，用"/"表示。

试题 11 (2017 年上半年试题 32)

在 Linux 中，可以使用___(32)___命令为计算机配置 IP 地址。

(32) A. ifconfig　　B. config　　C. ip-address　　D. ipconfig

参考答案：(32)A。

要点解析：配置主机网络接口命令为 ifconfig。主机网络接口配置包括：IP 地址、掩码和广播地址，以及高级的选项等。

试题 12 (2017 年上半年试题 33)

在 Linux 中，通常使用___(33)___命令删除一个文件或目录。

(33) A. rm-i　　B. mv-i　　C. mk-i　　D. cat-i

参考答案：(33)A。

要点解析：rm 命令提供删除文件的功能。

试题 13 (2017 年上半年试题 34)

在以太网中发生冲突时采用退避机制，___(34)___优先传输数据。

(34) A. 冲突次数最少的设备

B. 冲突中 IP 地址最小的设备

C. 冲突域中重传计时器首先过期的设备

D. 同时开始传输的设备

参考答案：(34)C。

要点解析：退避机制规定，在发生冲突时，由冲突域中重传计时器首先过期的设备优先传输数据。

试题 14 (2017 年上半年试题 35)

在 Windows 操作系统中，远程桌面使用的默认端口是___(35)___。

(35) A. 80　　B. 3389　　C. 8080　　D. 1024

参考答案：(35)B。

要点解析：80 为 HTTP 端口，用于网页浏览。1024 为 Reserved 端口，它是动态端口的开始。3389 为远程桌面使用的默认端口。8080 为代理端口，WWW 代理开发此端口。

试题 15 (2017 年上半年试题 36)

在 Linux 中，创建权限设置为-rw-rw-r--的普通文件，下面的说法中正确的是___(36)___。



(36) A. 文件所有者对该文件可读可写
B. 同组用户对该文件只可读
C. 其他用户对该文件可读可写
D. 其他用户对该文件可读可查询

参考答案：(36)A。

要点解析：-rw-rw-r--表示文件所有者可读可写，同组用户可读可写，其他用户只可读。

试题 16　(2017 年上半年试题 40)

在浏览器地址栏输入一个正确的网址后，本地主机将首先在__(40)__中查询该网址对应的 IP 地址。

(40) A. 本地 DNS 缓存　　B. 本机 hosts 文件
C. 本地 DNS 服务器　　D. 根域名服务器

参考答案：(40)A。

要点解析：域名查询记录：先查本地 DNS 缓存，再查 hosts 表，然后再查找本地 DNS 服务器，再之后查根域名服务器、顶级域名服务器、权限域名服务器。

试题 17　(2016 年下半年试题 30 和试题 31)

Windows 命令 tracert www.163.com.cn 显示的内容如图 8.45 所示，那么本地默认网关的 IP 地址是__(30)__，网站 www.163.com.cn 的 IP 地址是__(31)__。

```
C:\Documents and Settings\Administrator>tracert www.163.com.cn

Tracing route to www.163.com.cn [219.137.167.157]
over a maximum of 30 hops:

  1    26 ms    15 ms    11 ms  100.100.17.254
  2    <1 ms    <1 ms    <1 ms  254-20-168-128.cos.it-comm.net [128.168.20.254]

  3    <1 ms    <1 ms    <1 ms  61.150.43.65
  4    <1 ms    <1 ms    <1 ms  222.91.155.5
  5    <1 ms    <1 ms    <1 ms  125.76.189.81
  6     1 ms    <1 ms    <1 ms  61.134.0.13
  7    28 ms    28 ms    28 ms  202.97.35.229
  8    28 ms    29 ms    29 ms  61.144.3.17
  9    29 ms    29 ms    32 ms  61.144.5.9
 10    32 ms    32 ms    32 ms  219.137.11.53
 11    29 ms    29 ms    28 ms  219.137.167.157

Trace complete.
```

图 8.45　Windows 命令

(30) A. 128.168.20.254　　B. 100.100.17.254
C. 219.137.167.157　　D. 61.144.3.17

(31) A. 128.168.20.254　　B. 100.100.17.254
C. 219.137.167.157　　D. 61.144.3.17

参考答案：(30)B；(31)C。

要点解析：tracert 被称为 Windows 路由跟踪实用程序，在命令提示符 cmd 中使用该命令可以确定 IP 数据包访问目标时所选择的路径。tracert 第一跳为默认网关地址即 100.100.17.254。www.163.com.cn [219.137.167.157] 括号里的就是该网址的 IP 地址。

试题 18 (2016 年下半年试题 32)

在 Linux 系统中，要查看如下输出，可使用命令__(32)__。

```
Eth0 Link encap: Ethernet HWaddr 00:20:50:00:78:33
Inet addr:192.168.0.5 Bccast:192.168.0.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX:packets:9625272 errors:0 drogped:0 overruns:0 frame:0
TX:packets:6997276 errors:0 drogped:0 overruns:0 frame:0
Collisions:0 txqueuelen:100
Interrupt:19 Base address:0xc800
```

(32) A.[root@localhost]#ifconfig　　B. [root@localhost]#ipconfig　eth0
C. [root@localhost]#ipconfig　　D. [root@localhost]#ifconfig　eth0

参考答案：(32)A。

要点解析：如题输出显示的是网络设备的状态，而 ifconfig 就是 Linux 中用来配置主机网络接口的命令。

试题 19 (2016 年下半年试题 33)

当 DHCP 服务器拒绝客户端的 IP 地址请求时发送__(33)__报文。

(33) A. DhcpOffer　B. DhcpDecline　C. DhcpAck　D.DhcpNack

参考答案：(33)D。

要点解析：DhcpNack 是服务器无法正常分配 IP 时发送给客户端的报文，当 DHCP 服务器拒绝客户端的 IP 地址请求时发送 DhcpNack 报文。DhcpOffer 报文是服务器预提供 IP 的报文。DhcpDecline 报文是客户端发送给服务器的报文，通知所分配 IP 地址不可用。DhcpAck 报文是服务器发给客户端的报文，带有分配的 IP 的租期。此外 DhcpDiscover 报文是客户端发送给服务器请求 IP 租用的报文。DhcpRequest 是客户端确认使用 IP 发送给服务器的报文。DhcpRelease 报文是用于客户端释放 IP 地址发送给服务器的。

试题 20 (2016 年下半年试题 39)

在 Windows 的 DOS 窗口中输入命令

```
C:\>nslookup
>set type=a
>xyz.com.cn
```

这个命令序列的作用是__(39)__。

(39) A. 查询 xyz.com.cn 的邮件服务器信息
B. 查询 xyz.com.cn 到 IP 地址的映射
C. 查询 xyz.com.cn 的资源记录类型
D. 显示 xyz.com.cn 中各种可用的信息资源记录

参考答案：(39)B。

要点解析：每一个 DNS 服务器包含了它所管理的 DNS 命名空间的所有资源记录。资源记录包括和特定主机有关的信息，如 IP 地址、提供服务的类型等。常见的资源记录类型有 SOA(起始授权结构)、A(主机)、NS(名称服务器)、CNAME(别名)和 MX(邮件交换器)。A



记录也称为主机记录，是 DNS 名称到 IP 地址的映射，主要用于正向解析。

试题 21　(2016 年下半年试题 40)

下面是 DHCP 协议工作的 4 种消息，正确的顺序应该是 (40) 。

① DHCP　Discovery

② DHCP　Offer

③ DHCP　Request

④ DHCP　Ack

(40) A. ①③②④　　B.①②③④　　C.②①③④　　D.②③①④

参考答案：(40)B。

要点解析：DHCP 协议采用 UDP 作为传输协议，主机发送请求到 DHCP 服务器的 67 号端口，DHCP 服务器回应应答消息给主机的 68 号端口。

DHCP Client 以广播的方式发出 DHCP Discover 报文。

所有的 DHCP Server 都能够接收到 DHCP Client 发送的 DHCP Discover 报文，所有的 DHCP Server 都会给出响应，向 DHCP Client 发送一个 DHCP Offer 报文。

DHCP Client 只能处理其中的一个 DHCP Offer 报文，一般的原则是 DHCP Client 处理最先收到的 DHCP Offer 报文。

DHCP Client 会发出一个广播的 DHCP Request 报文，在选项字段中会加入选中的 DHCP Server 的 IP 地址和需要的 IP 地址。

DHCP Server 收到 DHCP Request 报文后，判断选项字段中的 IP 地址是否与自己的地址相同。如果不相同，DHCP Server 不做任何处理只清除相应 IP 地址分配记录；如果相同，DHCP Server 就会向 DHCP Client 响应一个 DHCP Ack 报文，并在选项字段中增加 IP 地址的使用租期信息。

DHCP Client 接收到 DHCP Ack 报文后，检查 DHCP Server 分配的 IP 地址是否能够使用。如果可以使用，则 DHCP Client 成功获得 IP 地址并根据 IP 地址使用租期自动启动续延过程；如果 DHCP Client 发现分配的 IP 地址已经被使用，则 DHCP Client 向 DHCP Server 发出 DHCP Decline 报文，通知 DHCP Server 禁用这个 IP 地址，然后 DHCP Client 开始新的地址申请过程。

DHCP Client 在成功获取 IP 地址后，随时可以通过发送 DHCP Release 报文释放自己的 IP 地址，DHCP Server 收到 DHCP Release 报文后，会回收相应的 IP 地址并重新分配。

试题 22　(2016 年下半年试题 41)

在 Linux 中， (41) 命令可将文件以修改时间顺序显示。

(41) A. Ls-a　　B. Ls-b　　C. Ls-c　　D. Ls-d

参考答案：(41)C。

要点解析：在 Linux 中，想要文件以修改时间的顺序显示，可以使用 Ls-c 命令。Ls-c 输出文件的 ctime(文件状态最后更改的时间)，并根据 ctime 排序。

试题 23　(2016 年下半年试题 42)

要在一台主机上建立多个独立域名的站点，下面的方法中 (42) 是错误的。

(42) A. 为计算机安装多块网卡　　B. 使用不同的主机头名
C. 使用虚拟目录　　D. 使用不同的端口号

参考答案：(42)C。

要点解析：在一台主机上建立多个独立域名的站点，可以使用：①不同的 IP 地址(多网卡)；②不同的端口号；③不同的主机头名。

虚拟主机之间相互独立，由用户自行管理。

试题 24　(2016 年下半年试题 46)

在 Windows Server 2003 中，__(46)__组成员用户具有完全控制权限。

(46) A. Users　　B. Power Users　　C. Administrators　　D. Guests

参考答案：(46)C。

要点解析：Administrators(管理员)组成员用户具有完全控制权限。

试题 25　(2016 年下半年试题 49)

从 FTP 服务器下载文件的命令是__(49)__。

(49) A. get　　B. dir　　C. put　　D. push

参考答案：(49)A。

要点解析：本题考查 FTP 协议及操作相基础知识。

FTP 命令由两条 TCP 连接来进行文件的上传和下载，FTP 服务器相应也有多条命令来对应，其中从 FTP 服务器下载文件的命令是 get。

试题 26　(2016 年上半年试题 35)

在 Linux 系统中，使用 Apache 服务器时默认的 Web 根目录是__(35)__。

(35) A. . . \htdocs　　B. /var/www/html
C. /var/www/usage　　D. . . \conf

参考答案：(35)B。

要点解析：Apache HTTP Server(简称 Apache)是 Apache 软件基金会的一个开放源代码的网页服务器，可以在大多数计算机操作系统中运行，由于其多平台和安全性被广泛应用，是最流行的 Web 服务器端软件之一。在 Linux 中，使用 Apache 服务器时默认的 Web 根目录是：/var/www/html。

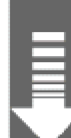
试题 27　(2016 年上半年试题 36)

下面关于 Linux 系统文件挂载的叙述中，正确的是__(36)__。

(36) A. /可以作为一个挂载点
B. 挂载点可以是一个目录，也可以是一个文件
C. 不能对一个磁盘分区进行挂载
D. 挂载点是一个目录时，这个目录必须为空

参考答案：(36)A。

要点解析：挂载点必须是一个目录。一个分区挂载在一个已存在的目录上，这个目录不为空，但挂载后这个目录下以前的内容将不可用。/根目录：存放系统命令和用户数据等(如果下面挂载点没有单独的分区，它们都将在根目录的分区中)。



试题 28　(2016 年上半年试题 50)

在 Windows 的 DOS 窗口中输入命令

```
C:\>nslookup
>settype=ptr
>211.151.91.165
```

这个命令序列的作用是 (50) 。

(50) A. 查询 211.151.91.165 的邮件服务器信息

B. 查询 211.151.91.165 到域名的映射

C. 查询 211.151.91.165 的资源记录类型

D. 显示 211.151.91.165 中各种可用的信息资源记录

参考答案：(50)B。

要点解析：PTR 记录也被称为指针记录，PTR 记录是 A 记录的逆向记录，作用是把 IP 地址解析为域名。

试题 29　(2015 年下半年试题 31)

在 Linux 系统中，使用 ifconfig 设置接口的 IP 地址并启动该接口的命令是 (31) 。

(31) A. ifconfig eth0 192.168.1.1 mask 255.255.255.0

B. ifconfig 192.168.1.1 mask 255.255.255.0 up

C. ifconfig eth0 192.168.1.1 mask 255.255.255.0 up

D. ifconfig 192.168.1.1 255.255.255.0

参考答案：(31)C。

要点解析：ifconfig 可以用来配置网络接口的 IP 地址、掩码、网关、物理地址等；值得一说的是用 ifconfig 为网卡指定 IP 地址，这只是用来调试网络，并不会更改系统关于网卡的配置文件。命令格式为：

```
ifconfig 网络端口 IP 地址 netmask 掩码地址 [up/down]
```

试题 30　(2015 年下半年试题 32)

在 Linux 系统中，在 (32) 文件中查看一台主机的名称和完整域名。

(32) A. etc/dev　　B. etc/conf　　C. etc/hostname　　D. etc/network

参考答案：(32)C。

要点解析：本题考查的是在 Linux 系统文件系统的基础知识。

在 Linux 操作系统中，TCP/IP 网络是通过若干文本文件进行配置的。系统在启动时通过读取一组有关网络配置的文件和脚本参数内容，来实现网络接口的初始化和控制过程，这些文件和脚本大多数位于/etc 目录下。

/etc/hostname 文件包含了 Linux 系统的主机名称，包括完全的域名。

/etc/host.conf 文件指定如何解析主机域名，Linux 通过解析器库来获得主机名对应的 IP 地址。

/etc/sysconfig/network 是一个用来指定服务器 h 的网络配置信息的文件，包含了控制和网络有关的文件和守护程序行为的参数。

试题 31 (2015 年下半年试题 39 和试题 40)

图 8.46 是配置某邮件客户端的界面，图中 a 处应填写__(39)__，b 处应填写__(40)__。

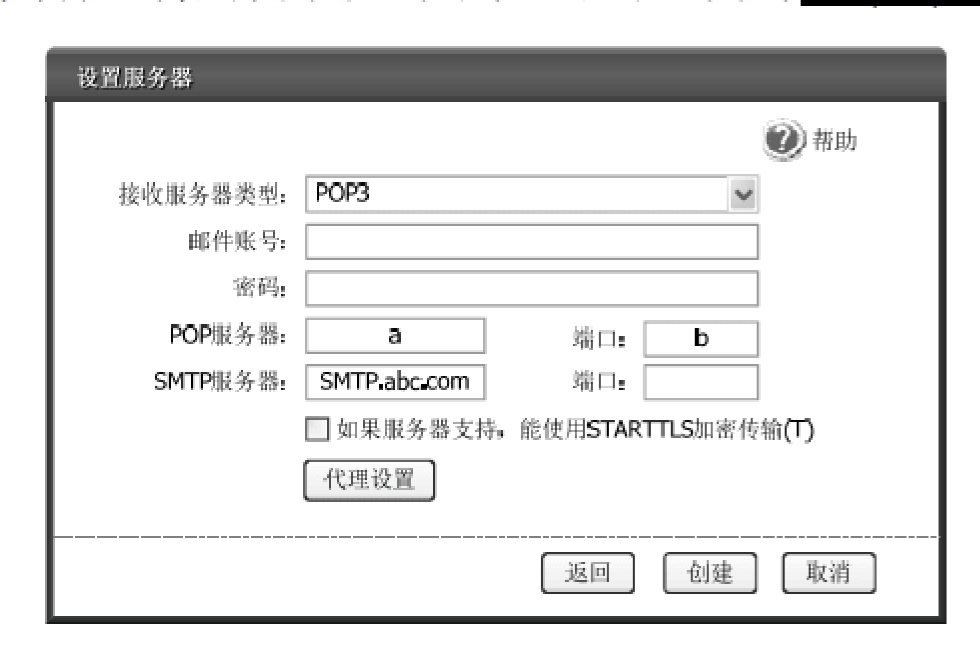


图 8.46 “设置服务器”对话框

(39) A. abc.com　　B. POP3.abc.com
C. POP.com　　D. POP3.com

(40) A. 25　　B. 52　　C. 100　　D. 110

参考答案：(39)B；(40)D。

要点解析：由图中 SMTP 服务器的域名 SMTP.abc.com 知道，邮件服务器所在主机的主机名为 abc.com，而接收服务器类型为 POP3，因此 a 处填入 POP3.abc.com。在 TCP/IP 协议下，POP3 协议分配的端口号为 110，因此 b 处填入 110。

8.3.2 案例分析试题

试题 1 (2017 年下半年下午试题三)

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】

某公司有两个办事处，分别利用装有 Windows Server 2008 的双宿主机实现路由功能，此功能由 Windows Server 2008 中的路由和远程访问服务来完成。管理员分别为这两台主机中的一个网卡配置了不同的 IP 地址，如图 8.47 所示。

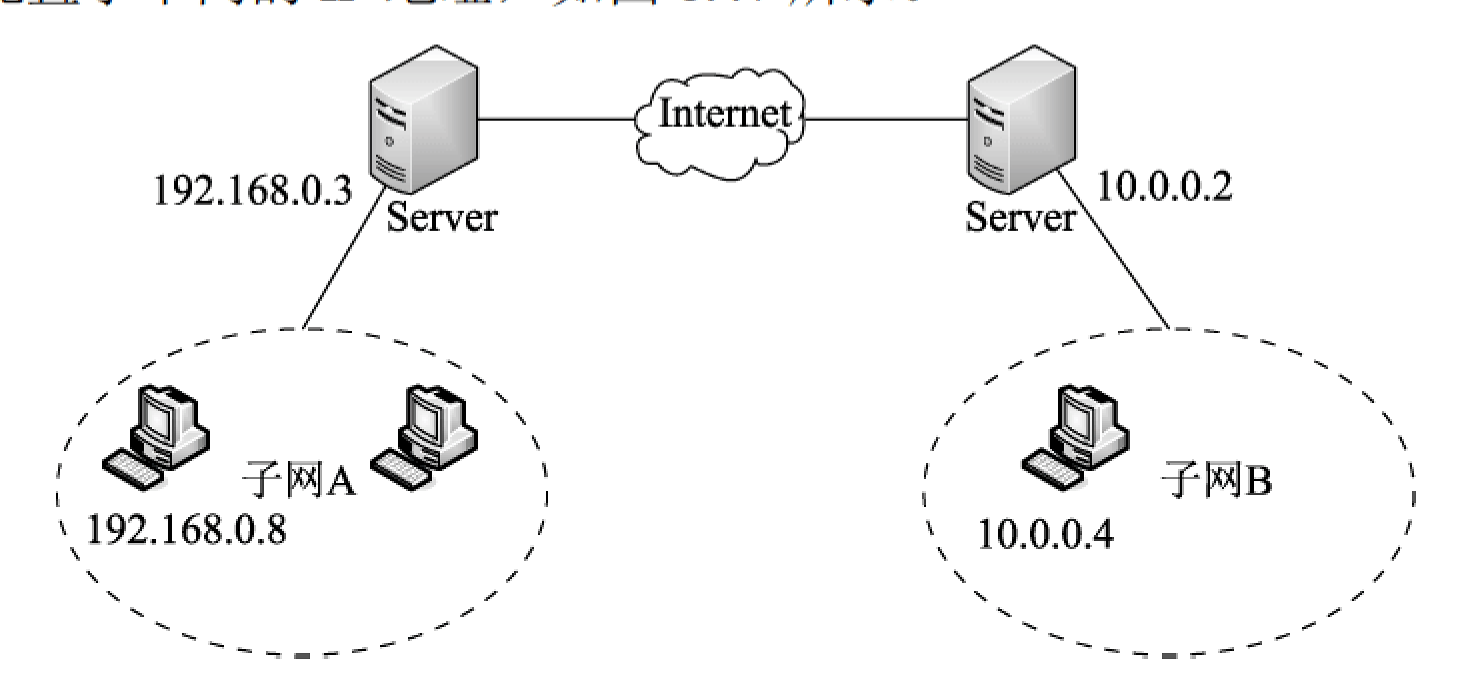


图 8.47 配置 IP 地址

【问题 1】(4 分)

在“管理您的服务器”中单击“添加或删除角色”，此时应当在服务器角色中选择__(1)__

来完成路由和远程访问服务的安装。在下列关于路由和远程访问服务的选项中，不正确的是__(2)__。

(1)备选答案：

A. 文件服务器　　B. 应用程序服务器(IIS，ASP.NET)

C. 终端服务器　　D. 远程访问/VPN 服务

(2)备选答案：

A. 可连接局域网的不同网段或子网，实现软件路由器的功能

B. 把分支机构与企业网络通过 Intranet 连接起来，实现资源共享

C. 可使远程计算机接入企业网络中访问网络资源

D. 必须通过 VPN 才能使远程计算机访问企业网络中的网络资源

【问题 2】(4 分)

两个办事处子网的计算机安装 Windows 7 操作系统，要实现两个子网间的通信，子网 A 和子网 B 中计算机的网关分别为__(3)__和__(4)__。子网 A 中的计算机用 ping 命令来验证数据包能否路由到子网 B 中，图 8.48 中参数使用默认值，从参数__(5)__可以看出数据包经过了__(6)__个路由器。

```
C:\>ping 10.0.0.4
Pinging 10.0.0.4 with 32 bytes of data:
Reply from 10.0.0.4: bytes=32 time=10ms TTL=122
Reply from 10.0.0.4: bytes=32 time<10ms TTL=122
Reply from 10.0.0.4: bytes=32 time<10ms TTL=122
Reply from 10.0.0.4: bytes=32 time<10ms TTL=122

Ping statistics for 10.0.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 <0% loss>,
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average =  2ms
```

图 8.48　参数设置

(3)备选答案：

A. 192.168.0.0　　B.192.168.0.1　　C.192.168.0.3　　D. 无须配置网关

(4)备选答案：

A. 10.0.0.0　　B.10.0.0.1　　C.10.0.0.2　　D. 无须配置网关

(5)备选答案：

A. bytes　　B.time　　C.TTL　　D. Lost

【问题 3】(8 分)

Windows Server 2008 支持 RIP 动态路由协议。在 RIP 接口属性页中，如果希望路由器每隔一段时间向自己的邻居广播路由表以进行路由信息的交换和更新，则需要在“操作模式”中选择__(7)__。在“传出数据包协议”中选择__(8)__，使网络中其他运行不同版本的邻居路由器都可接受此路由器的路由表；在“传入数据包协议”中选择__(9)__，使网络中其他运行不同版本的邻居路由器都可向此广播路由表。

(7)备选答案：

A. 周期性的更新模式　　B. 自动-静态更新模式

(8)备选答案：

A. RIPv1 广播　　B. RIPv2 多播　　C.RIPv2 广播

(9)备选答案：

A. 只是 RIPv1　　B. 只是 RIPv2

C. RIPv1 和 v2　　D. 忽略传入数据包

为了保护路由器之间的安全通信，可以为路由器配置身份验证。选中“激活身份验证”复选框，并在“密码”文本框中输入一个密码。所有路由器都要做此配置，所配置的密码 __(10)__。

(10)备选答案：

A. 可以不同　　B. 必须相同

【问题 4】(4 分)

由于在子网 A 中出现病毒，需在路由接口上启动过滤功能，不允许子网 B 接收来自子网 A 的数据包，在选择入站筛选器且筛选条件是“接收所有除符合下列条件以外的数据包”时，如图 8.49 所示，由源网络 IP 地址和子网掩码得到的网络地址是 __(11)__，由目标网络 IP 地址和子网掩码得到的网络地址是 __(12)__，需要选择协议 __(13)__。如果选择协议 __(14)__，则会出现子网 A 和子网 B 之间 ping 不通但是子网 B 能接收来自子网 A 的数据包的情况。

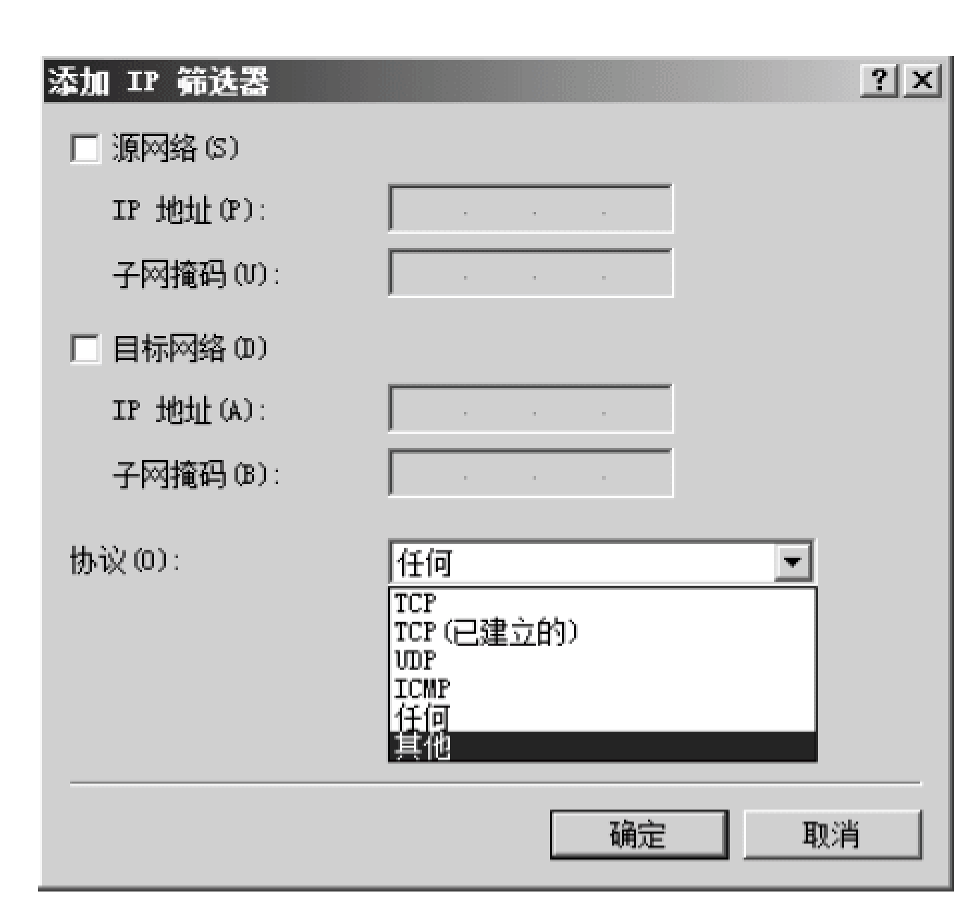


图 8.49　“添加 IP 筛选器”对话框

(11)备选答案：

A. 192.168.0.0　　B. 192.168.0.1　　C. 192.168.0.3　　D. 192.168.0.8

(12)备选答案：

A. 10.0.0.0　　B. 10.0.0.1　　C. 10.0.0.3　　D. 10.0.0.4

(13)、(14)备选答案：

A. ICMP　　B. TCP　　C. UDP　　D. 任何

参考答案：

【问题 1】(1)D；(2)D。

【问题 2】(3)C；(4)C；(5)C；(6)133。





【问题 3】(7)A；(8)A；(9)C；(10)B。

【问题 4】(11)A；(12)D；(13)D；(14)A。

要点解析：

【问题 1】在 Windows 系统中，要想实现路由和远程访问服务需要以管理员身份登录，打开控制面板，运行“添加和删除程序”命令，选择“添加或删除 Windows 组件”，启动 Windows 组件向导，选择“远程访问/VPN 服务”即可。

针对普通用户的远程访问需求，较为常见的方式有 3 类。

第一类是直接开放内部应用系统的端口，允许外部 IP 直接访问，通过应用系统自身的账号验证机制防范非法用户。

第二类是利用 Windows Server 2003 及更新的版本所提供的 Terminal Service 功能，在外部 PC 上运行 Windows 远程桌面，先连接到内网的 Terminal Server，再通过该 Server 代理访问内网应用系统。

第三类是采用 VPN 技术实现与企业内网的远程连接，进而在 VPN 中访问内网应用系统。因此 VPN 并不是远程计算机访问企业网络的唯一途径，并不是必须通过 VPN。

【问题 2】通过文字及图形说明，可知子网 A 连接在 192.168.0.0 网段，而子网 B 处在 10.0.0.0 网段，对应的网关地址分别为网段连接的服务器 IP。ping 命令通常用于测试连通性，其中 TTL 值代表跳数，以 255 跳开始，每经过一个路由器，就会减 1。

【问题 3】为支持 RIP 动态路由协议，可配置相应的 RIP 版本，RIP 有两个版本，v1 只支持有类别路由信息，并以广播的形式发送整个路由表给邻居；v2 支持无类别路由，以组播的方式发送整个路由表信息进行路由收敛。在“操作模式”中选择“周期性的更新模式”，这样，在缺省的情况下每隔 30 秒此路由器会向自己的邻居广播自己的路由表以进行路由信息的交换和更新。在“传出数据包协议”中选择“RIPv1 广播”，当网络中有 RIPv1 时默认选择该版本。在“传入数据包协议”中选择“RIP1 和 2 版”。这样可以使网络中其他运行 RIP 版本 1 和版本 2 的邻居路由器都可以向此路由器广播路由表。为了确保路由器之间的安全通信，可在路由器和路由器之间增加身份验证，并且相互连接的双方密码信息要一致。

【问题 4】出现两个网络之间 ping 不通但是其中一个网络能接收来自另一个网络的数据包的情况，一般是采用了 ICMP 协议，ICMP 协议对于网络安全具有极其重要的意义。ICMP 协议本身的特点决定了它非常容易被用于攻击网络上的路由器和主机。

试题 2 (2017 年上半年下午试题三)

阅读以下说明，回答问题 1 至问题 3，将解答填入答题纸对应的解答栏内。

【说明】

请根据 Windows 服务器的安装与配置，回答下列问题。

【问题 1】(共 8 分)

图 8.50 是安装好的服务器管理器界面，在当前配置下，根域的名称是__(1)__。

图示中角色服务配置时，建立域控制器 DC(Domain Controller)，需要通过命令行方式运行__(2)__命令；域中的 DC 和 DNS 配置在同一设备时，需要将独立服务器的首个 DNS 与 DC 的 IP 地址配置为__(3)__；DHCP 服务加入 DC 需要__(4)__，否则服务报错。

(2)备选答案：

A. dcomcnfg　　　　B. dcpromo

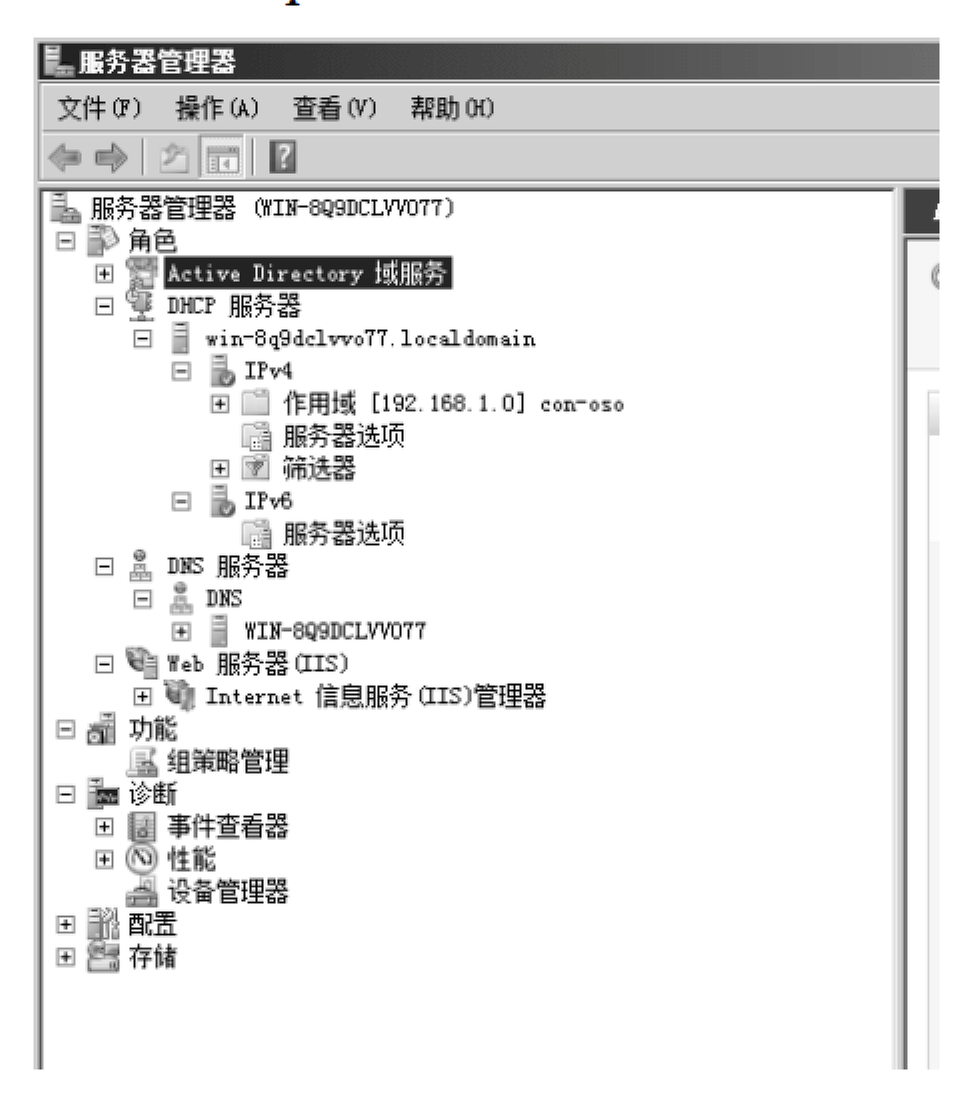
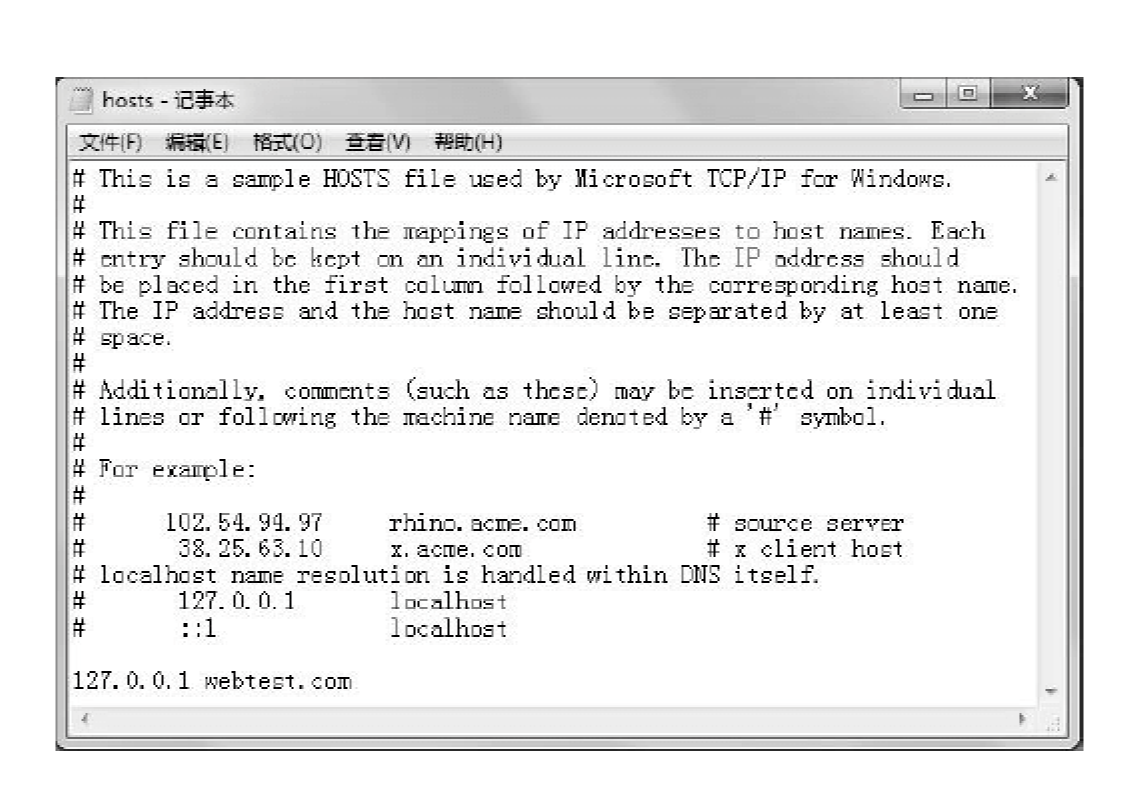


图 8.50　服务器管理器界面

【问题 2】(共 6 分)

图 8.51 是 hosts 文件内容，图 8.52 是配置安全站点 https://webtest.com 的界面。



hosts - 记事本

文件(F)　编辑(E)　格式(O)　查看(V)　帮助(H)

```
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host
# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost

127.0.0.1 webtest.com
```



图 8.51　host 文件内容　　　　图 8.52　配置安全站点的界面

图 8.51 中，127.0.0.1 webtest.com 的含义是＿(5)＿。在建立安全站点时，需要在 Web 服务器上启用＿(6)＿功能，并且绑定创建好的证书。

(6)备选答案：

A. SSL　　　　B. 代理

若将图 8.52 中 https 的端口号改为 8000，访问站点的 URL 是＿(7)＿。

【问题 3】(共 6 分)

图 8.53 是通过设备管理器查看到的信息，未安装驱动程序的设备提供＿(8)＿功能。

在“驱动程序”选项卡中会显示驱动程序提供商、驱动程序日期、驱动程序版本和＿(9)＿信息。

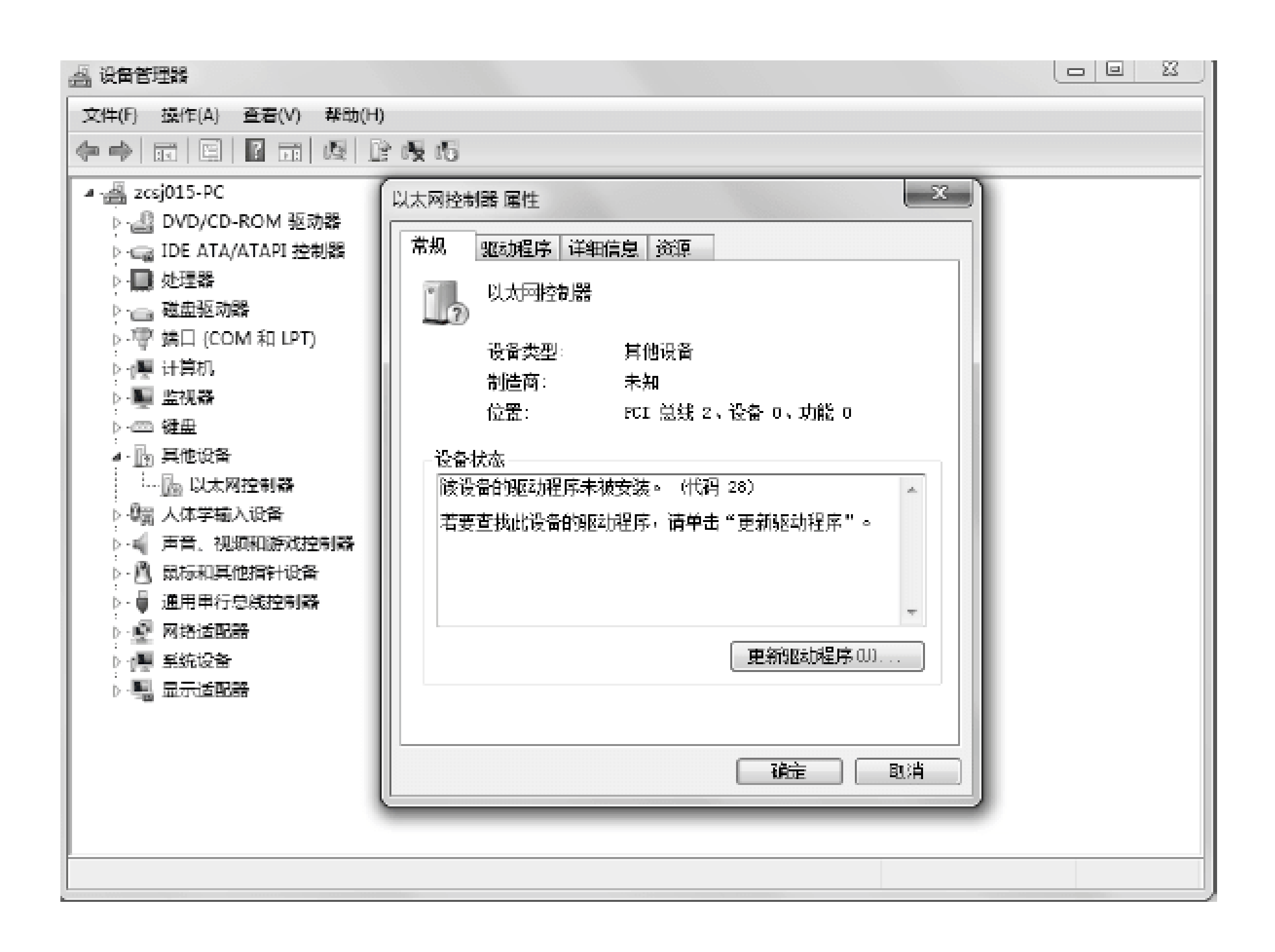


图 8.53　设备管理器

若更新驱动程序后无法正常运行，可以在该选项卡页面通过__(10)__操作将以前的驱动程序恢复。

(9)备选答案：

A. 数字签名　　　　　　B. 硬件类型

参考答案：

【问题 1】(1)con-oso.com；(2)B；(3)一样；(4)授权。

【问题 2】(5)在主机 hosts 表中建立 webtest.com 和 127.0.0.1 的对应关系；(6)A；(7)https://webtest.com:8000。

【问题 3】(8)更新驱动程序；(9)A；(10)回退驱动程序。

要点解析：

【问题 1】con-oso.com 域林中第一个域树的名字就是根域的名字；dcomcnfg 命令用于开启“组件服务”配置；dcpromo 命令用于将服务器提升为域控制器，或者将域控制器降级为成员服务器，dcpromo 是 Windows 做域控制器的开关命令；题意 DNS 和 DC 的 IP 需要建立一种对应关系；加入 DC 控制域必须授权。

【问题 2】访问 webtest.com，解析出 IP 为 127.0.0.1 相当于 DNS 的映射，当主机访问这个域名时会先到本机 host 文件找到这条记录解析成 127.0.0.1；安全站点 SSL 是 TCP 和应用层的安全协议通过数字证书加密建立安全站点绑定创建好的证书，SSL 可以对万维网客户与服务器之间传送的数据进行加密和鉴别。在双方握手阶段，对将要使用的加密算法和双方共享的会话密钥进行协商，完成客户与服务器之间的鉴别。在握手完成后，所传送的数据都使用会话密钥进行传输，以保证站点的安全性；默认的端口 443 是可以直接访问的，如果需要修改端口号访问，方法是域名后边加“：”端口号。

【问题 3】设备管理器是一种管理工具，可用它来管理计算机上的设备。可以使用“设备管理器”查看和更改设备属性、更新设备驱动程序、配置设备设置和卸载设备。在“驱动程序”选项卡中会显示驱动程序提供商、驱动程序日期、驱动程序版本和数字签名信息，打开窗口即可看到；通过回滚驱动程序，可以回到原来的驱动版本上。

试题 3 (2016 年下半年下午试题三)

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】

某公司的 IDC(互联网数据中心)服务器 Server1 采用 Windows Server 2003 操作系统，IP 地址为 172.16.145.128/24，为客户提供 Web 服务和 DNS 服务；配置了三个网站，域名分别为 www.companyl.com、www.company2.com 和 www.company3.com，其中 company1 使用默认端口。基于安全的考虑，不允许用户上传文件和浏览目录。company1.com、company2.com 和 company3.com 对应的网站目录分别为 Company1-web、Company2-web 和 Company3-web，如图 8.54 所示。

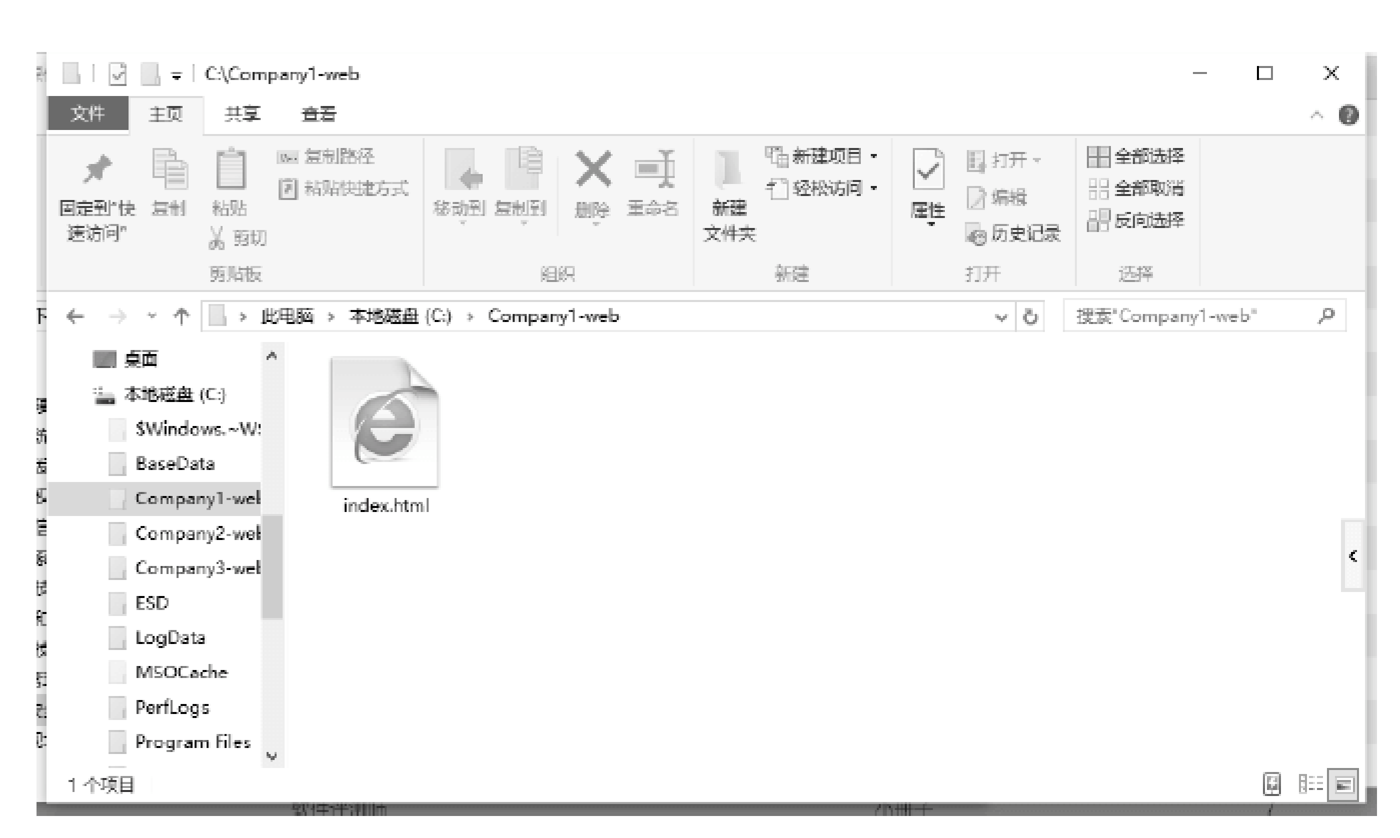


图 8.54　网站目录

【问题 1】(2 分，每空 1 分)

为安装 Web 服务和 DNS 服务，Server1 必须安装的组件有__(1)__、__(2)__。

(1)、(2)备选答案：

A. 网络服务　　B. 应用程序服务器　　C. 索引服务

D. 证书服务　　E. 远程终端

【问题 2】(4 分，每空 2 分)

在 IIS 中创建这三个网站时，在图 8.55 中勾选读取、__(3)__和执行，并在图 8.56 的“文档”选项卡中添加__(4)__为默认文档。

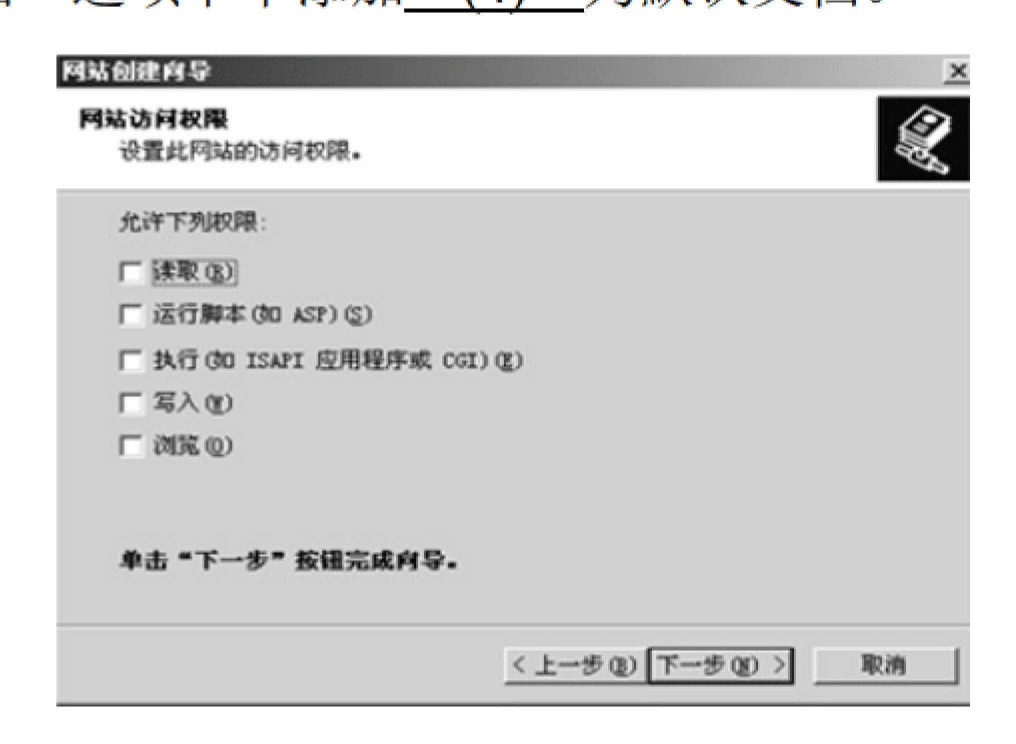


图 8.55　网站创建向导



图 8.56　“文档”选项卡

【问题 3】(6 分，每空 1 分)

1. 为了节省成本，公司决定在一台计算机上为多类用户提供服务。使用不同端口号来区分不同网站，company1 使用默认端口__(5)__，company2 和 company3 的端口应在 1025 至__(6)__范围内任意选择，在访问 company2 或者 company3 时需在域名后添加对应端口号，使用__(7)__符号连接。设置完成后，管理员对网站进行了测试，测试结果如图 8.57 所示，原因是__(8)__。



图 8.57　测试结果

(8)备选答案：

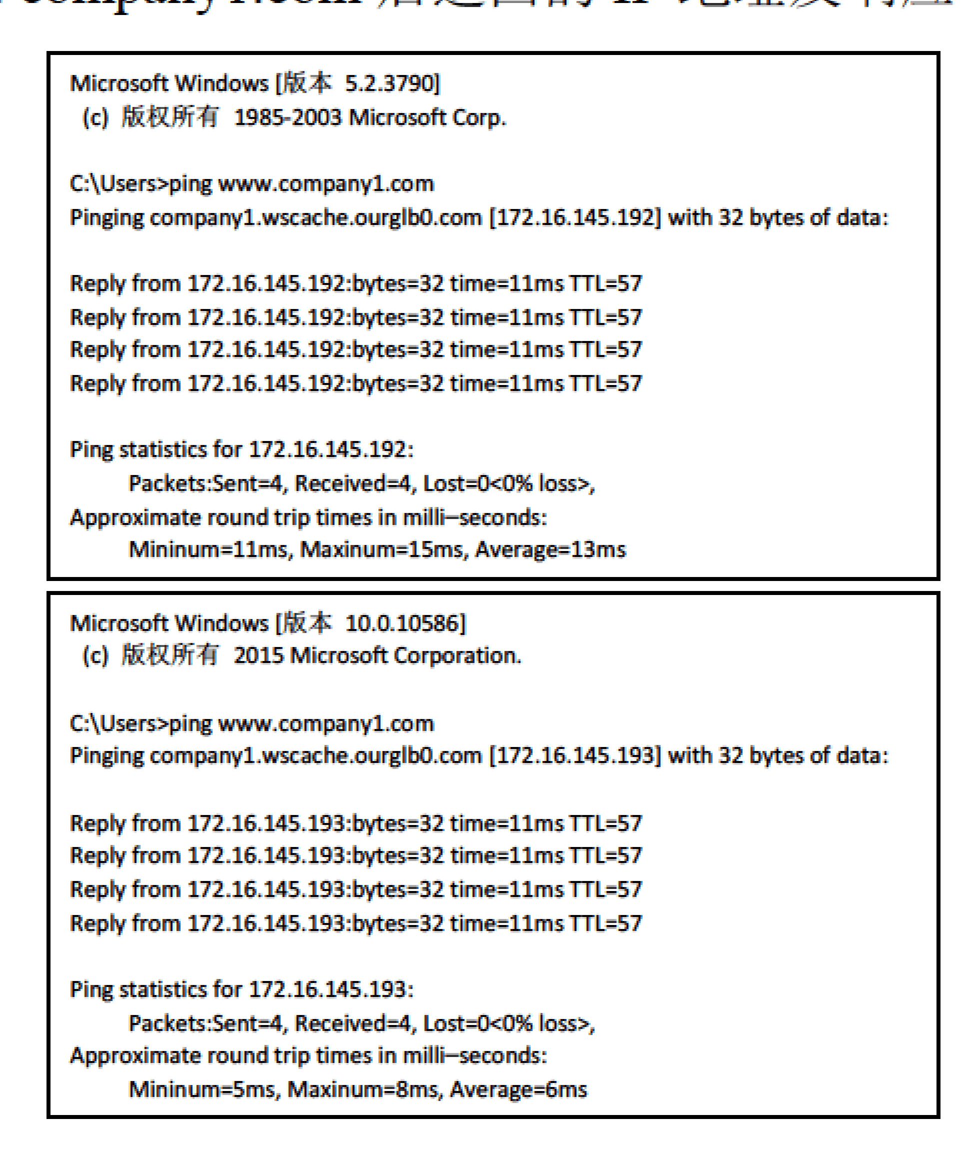
A. IP 地址对应错误　　　　B. 未指明 company1 的端口

C. 未指明 company2 的端口　　D. 主机头设置错误

2. 为便于用户访问，管理员决定采用不同主机头值的方法为用户提供服务，需在 DNS 服务中正向查找区域为三个网站域名分别添加__(9)__记录。网站 company2 的主机头值应设置为__(10)__。

【问题 4】(8 分，每空 2 分)

随着 company1 网站访问量的不断增加，公司为 company1 设立了多台服务器。下面是不同用户 ping 网站 www. company1.com 后返回的 IP 地址及响应状况，如图 8.58 所示。



```
Microsoft Windows [版本 5.2.3790]
 (c) 版权所有 1985-2003 Microsoft Corp.

C:\Users>ping www.company1.com
Pinging company1.wscache.ourglb0.com [172.16.145.192] with 32 bytes of data:

Reply from 172.16.145.192:bytes=32 time=11ms TTL=57
Reply from 172.16.145.192:bytes=32 time=11ms TTL=57
Reply from 172.16.145.192:bytes=32 time=11ms TTL=57
Reply from 172.16.145.192:bytes=32 time=11ms TTL=57

Ping statistics for 172.16.145.192:
      Packets:Sent=4, Received=4, Lost=0<0% loss>,
Approximate round trip times in milli-seconds:
      Mininum=11ms, Maxinum=15ms, Average=13ms
```

```
Microsoft Windows [版本 10.0.10586]
 (c) 版权所有 2015 Microsoft Corporation.

C:\Users>ping www.company1.com
Pinging company1.wscache.ourglb0.com [172.16.145.193] with 32 bytes of data:

Reply from 172.16.145.193:bytes=32 time=11ms TTL=57
Reply from 172.16.145.193:bytes=32 time=11ms TTL=57
Reply from 172.16.145.193:bytes=32 time=11ms TTL=57
Reply from 172.16.145.193:bytes=32 time=11ms TTL=57

Ping statistics for 172.16.145.193:
      Packets:Sent=4, Received=4, Lost=0<0% loss>,
Approximate round trip times in milli-seconds:
      Mininum=5ms, Maxinum=8ms, Average=6ms
```

图 8.58　响应状况

从图 8.58 可以看出，域名 www.company1.com 对应了多个 IP 地址，说明在图 8.59 所示的 DNS 属性中启用了__(11)__功能。

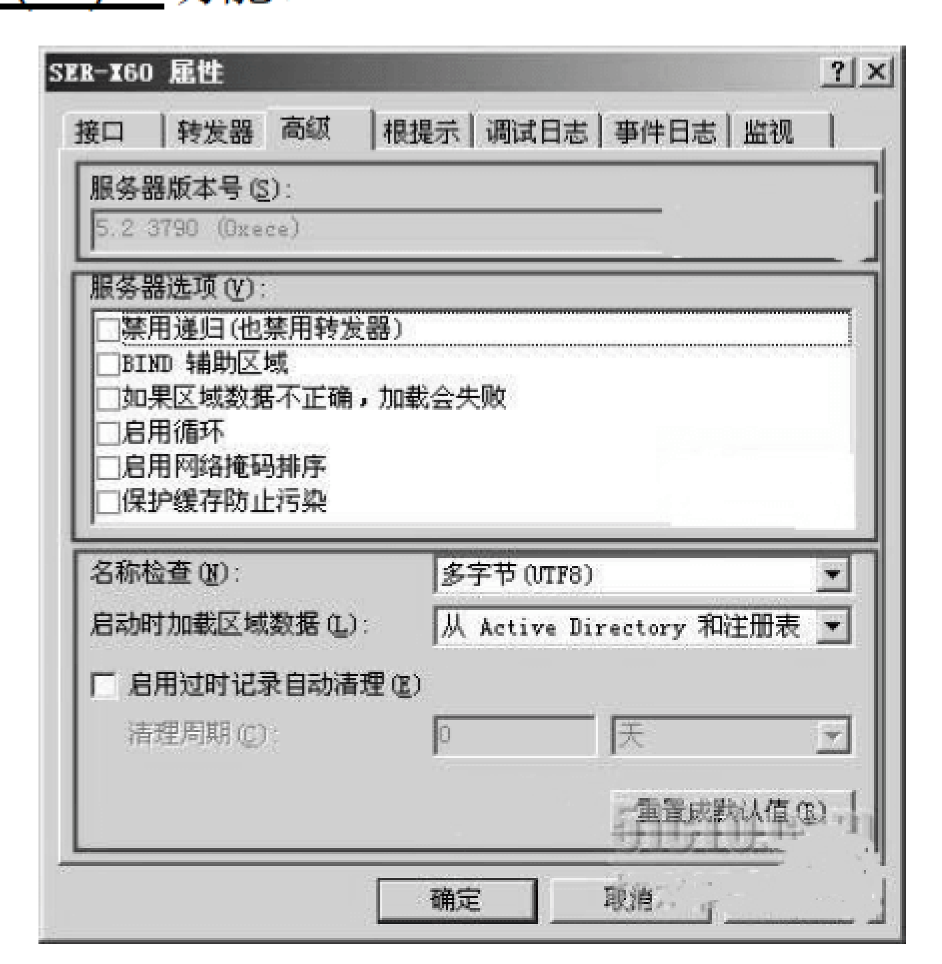


图 8.59 “SER-X60 属性”对话框

在图 8.59 中选中“启用网络掩码排序”复选框后，当存在多个匹配记录时，系统会自动检查这些记录与客户端 IP 的网络掩码匹配度，按照__(12)__原则来应答客户端的解析请求。如果选中“禁用递归(也禁用转发器)”复选框，这时 DNS 服务器仅采用__(13)__查询模式。当同时启用了网络掩码排序和循环功能时，__(14)__优先级较高。

(14)备选答案：

A. 循环　　　　B. 网络掩码排序

参考答案：

【问题 1】(1)A；(2)B (答案顺序可互换)。

【问题 2】(3)运行脚本(如 ASP)(S)；(4) index.html。

【问题 3】(5)80；(6)65535；(7) :；(8)C；(9)A(DNS 的 A 记录)；(10) www.company2.com。

【问题 4】(11)循环；(12)掩码接近度匹配对访问者实现的本地子网优先级排序；(13)迭代；(14)B。

要点解析：

【问题 1】出于对服务器安全性的着想，微软取消了安装操作系统时默认安装相关 Windows 组件的做法，因此安装 Web 服务和 DNS 服务，Server1 需要分别在“Windows 组件向导”中选中“应用服务器”和“网络服务”复选框，而后才能进行相关配置。

【问题 2】从题目中“不允许用户上传文件和浏览目录”可见访问权限设置中，不能选择“写入”和“浏览”权限。

默认文档：它是指在访问网站的时候自动定位的一个首先访问页面文件。本题中的网站主目录中只有一个文件 index.html，而“文档”选项卡中无此文档，所以需要手工添加。

【问题 3】Web 服务的默认端口是 80，在一台计算机上建立多站点，可以使用不同 IP 地址、不同主机头、不同端口号三种方式，其中：采用端口号区分不同站点。对于非标准端口，在访问时需要在域名或 IP 地址后面加上“:端口号”，如 www. company2.com:8080。

用不同主机头值的方法时，需要在 DNS 中为每个网站的域名添加主机记录，对于 IP 地址是同一个地址，每个站点的主机头设置为这个站点的完整域名，如网站 company2 的主机头值设置为：www. company2.com。采用主机头区分站点在访问时不能通过 IP 地址，只能通过域名的方式访问。

【问题 4】DNS 轮询就是指 DNS 服务器将域名解析请求按照 A 记录的顺序，逐一分配到不同的 IP 上，同时在一定程度上也实现了简单的负载均衡。

网络掩码排序可以根据本地子网优先级来判断 DNS 地址和客户端是否在同一个网段或者离得比较近，然后优先返回较近的服务器的地址。

关于本地子网优先级：

当集群中的服务器不在同一网段时，默认情况下，当客户机查询解析映射到多个 IP 地址的主机名时，DNS 服务使用本地子网优先排序作为给出同一网络上首选 IP 地址的方法。此功能要求客户应用程序尝试使用连接可用的最近(一般是最快的)IP 地址连接至主机。

DNS 服务按以下方式使用本地子网优先级。

① DNS 服务确定是否需要本地子网的优先级排序查询响应。

如果有多个地址资源记录与要查询的主机名匹配，则 DNS 服务可按其子网位置重新对记录进行排序。如果查询的主机名只与一个地址资源记录匹配，或者客户机的 IP 网络地址与多重资源记录响应列表上的任何映射地址的 IP 网络地址匹配，则不需要进行优先排列。

② 对于匹配响应列表中的每一个资源记录，DNS 服务决定了哪些记录(如果有)与查询客户机的子网位置匹配。

③ DNS 服务重新对响应列表进行排序，以便将与发出请求的客户机的本地子网匹配的主机地址资源记录排在响应列表中的第一位。

④ 按子网的顺序进行优先级排序后，响应列表将返回给发出请求的客户机。

当同时启用网络掩码排序和启用循环功能时，启用网络掩码排序的优先级比启用循环功能的优先级更高，此时，启用循环只是作为启用网络掩码排序结果的辅助方式。如果启用网络掩码排序在匹配客户端解析请求的资源记录中找到了匹配客户端子网 ID 的资源记录，则对其他非匹配的资源记录进行循环排序，否则将对所有匹配客户端解析请求的资源记录进行循环排序。

DNS 查询分为递归和迭代两种模式，本题中禁用递归，则必然是使用迭代查询模式。

试题 4 (2016 年上半年下午试题三)

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】

某企业采用 Windows Server 2003 配置了 DHCP、DNS 和 Web 服务。

【问题 1】(每空 1 分，共 4 分)

DHCP 服务器地址池 192.168.0.1～192.168.0.130，其中 192.168.0.10 分配给网关，192.168.0.11～192.168.0.15 分配给服务器，192.168.0.20 分配给网络管理员。

请填充图 8.60～图 8.62 中(1)～(4)处空缺内容。

【问题 2】(每空 1.5 分，共 9 分)

DNS 的配置如图 8.63 所示。

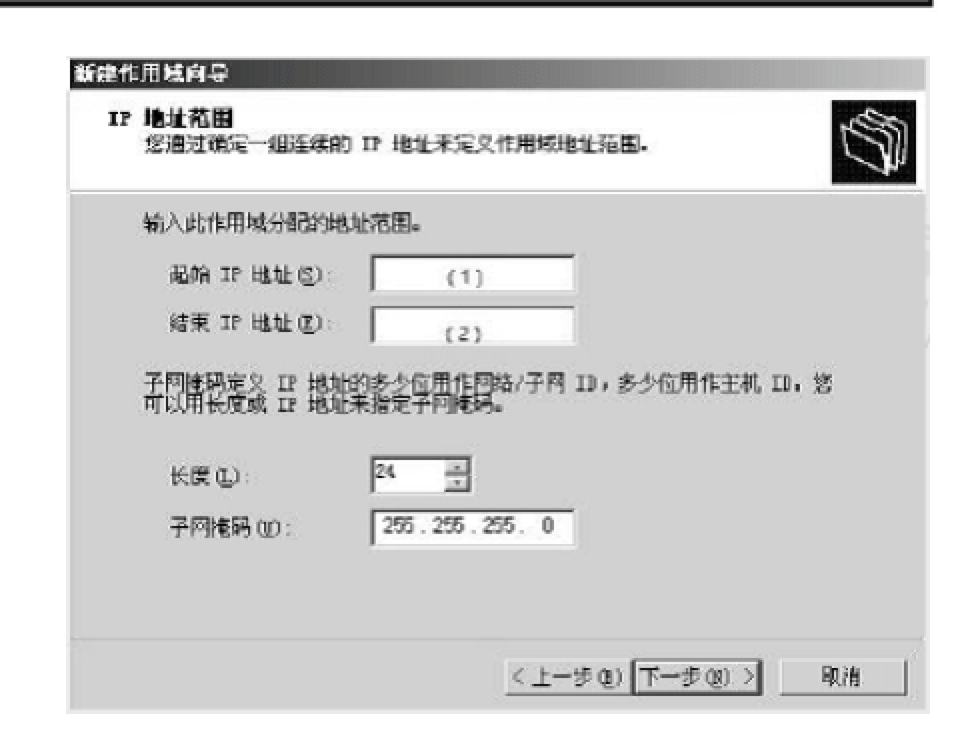


图 8.60　IP 地址范围

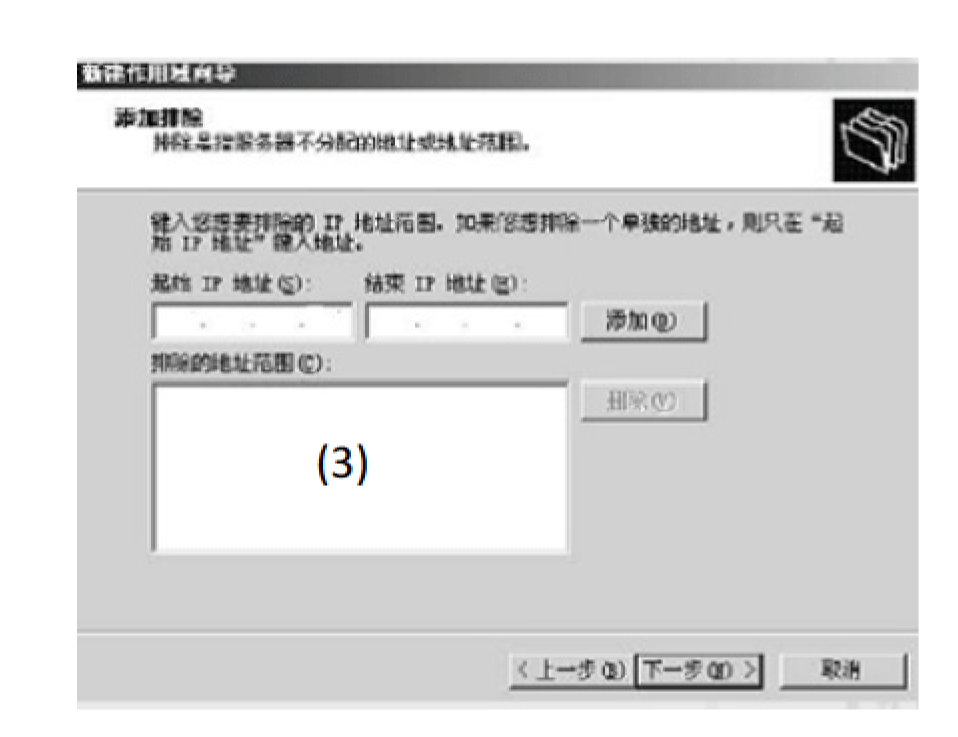


图 8.61　添加排除



图 8.62　“新建保留”对话框

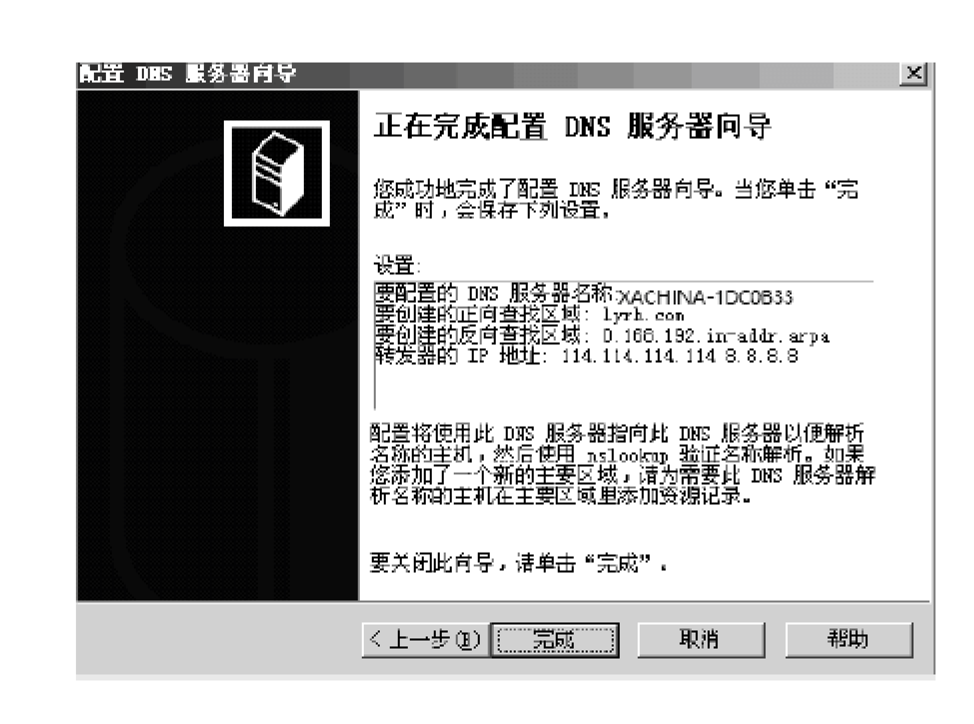


图 8.63　DNS 的配置

根据图 8.63 判断正误(正确的答“对”，错误的答“错”)。

A. XACHINA-1DC0B33 的 IP 地址为 114.114.114.114。__(5)__

B. 该域名服务器无法解析的域名转发到 114.114.114.114 或 8.8.8.8。__(6)__

C. 域 lyrh. com 的资源记录包含在该 DNS 服务器中。__(7)__

D. 客户机的“首选 DNS 服务器”地址必须与该 DNS 服务器地址一致。__(8)__

E. 该域名服务器是 lyrh. com 的授权域名服务器。__(9)__

F. 该域名服务器支持 192.168.101.6 地址的反向域名查找。__(10)__

【问题 3】(每空 2 分，共 4 分)

Web 服务器的配置如图 8.64 所示。

1. 如图 8.64 所示，通过主机头的方式建立两个网站 www. ycch. com 和 www. lyrh. com，网站配置是__(11)__。



图 8.64　Web 服务器的配置





(11)备选答案：

A. 相同的 IP 地址，不同的端口号　　B. 不同的 IP 地址，相同的目录

C. 相同的 IP 地址，不同的目录　　D. 相同的主机头，相同的端口号

2. 除了主机头方式，还可以采用__(12)__方式在一台服务器上配置多网站。

【问题 4】(每空 1 分，共 3 分)

Windows Server 2003 管理界面如图 8.65 所示。

1. 图 8.65 中设备打黄色“！”的含义是__(13)__，设备打“↓”的含义是__(14)__。

2. 图 8.65 中 1394 网络适配器能连接什么设备？__(15)__。

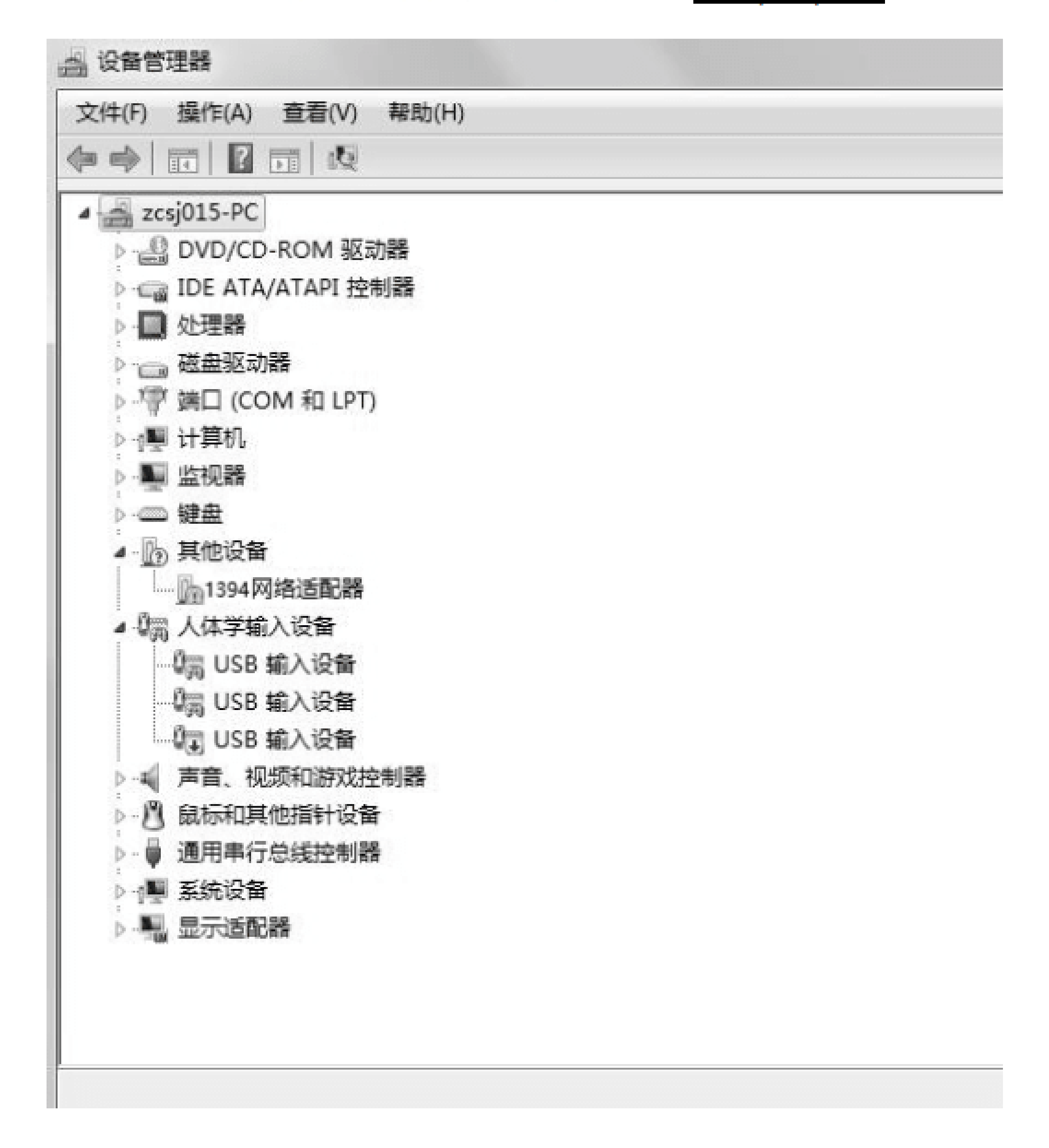


图 8.65　管理界面

参考答案：

【问题 1】

(1)192.168.0.1；

(2)192.168.0.130；

(3)192.168.0.10-192.168.0.15 以及 192.168.0.20；

(4)192.168.0.20。

【问题 2】

(5)错；(6)对；(7)对；(8)错；(9)对；(10)错。

【问题 3】

(11)C。

(12)不同的 IP 地址、相同的 IP 但不同的端口号。

【问题 4】

(13)硬件未被操作系统识别、设备驱动程序尚未安装。

(14)设备被禁用。

(15)连接外部视频设备。

要点解析：

【问题1】新建作用域，该作用域分配的IP地址范围也就是DHCP服务器地址池的地址范围192.168.0.1～192.168.0.130。

图8.57中要求服务器不分配的地址，由题意知192.168.0.10分配给网关，192.168.0.11～192.168.0.15分配给服务器，以及192.168.0.20分配给网络管理员，故192.168.0.10～192.168.0.15和192.168.0.20均排除。

(4)空是新建保留，把IP固定分配给某台主机，也就是分配给网络管理员的地址192.168.0.20。

【问题2】A:114.114.144.144是转发域名服务器的地址。

B:只要是本域名服务器无法解析的地址应首先查找转发域名服务器，也就是114.114.114.144和8.8.8.8。

C:该服务器创建了lyrh. Com的正向查找区域，所以显然包括相应的资源记录。

D:客户机用的DNS服务器和这个域名服务器无关。

E:该DNS服务器是lyrh.com的授权域名服务器。

F:只能支持192.168.0.x的地址反向域名查找。

【问题3】在大多数情况下，若要在一台服务器上架设多个Web网站，需要用到虚拟主机技术。IIS通过分配TCP端口、IP地址和主机头名来在一个服务器上运行多个网站。虚拟主机之间是相互独立的，由用户自行管理。该方法可以节约硬件投资，节省空间，降低成本。

(1) 基于附加TCP端口架设多个Web网站。

使用格式为http://域名:端口的网址来访问的网站实际上是利用TCP端口号，在同一服务器上架设不同网站。

(2) 基于不同的IP地址架设多个网站。

将每个网站绑定到不同的IP地址，以确保每个网站域名对应于独立的IP地址。

(3) 基于主机头名架设多个Web网站。

由于传统的IP虚拟主机浪费IP地址，在实际的应用中一般更倾向于采用非IP虚拟主机技术，也就是把多个域名的主机头名绑定到同一IP。

【问题4】在设备管理器中，黄色的问号表示该硬件没有能够被操作系统识别、没有安装驱动程序；感叹号则表示驱动程序安装得不正确；红色的×号则表示该设备已停用。

1394网络适配器主要连接视频设备，有视频采集之作用。

试题5 (2015年下半年下午试题三)

【说明】

某企业采用Windows Server 2003配置了Web、FTP和邮件服务。

【问题1】(4分)

Web的配置如图8.66和图8.67所示。

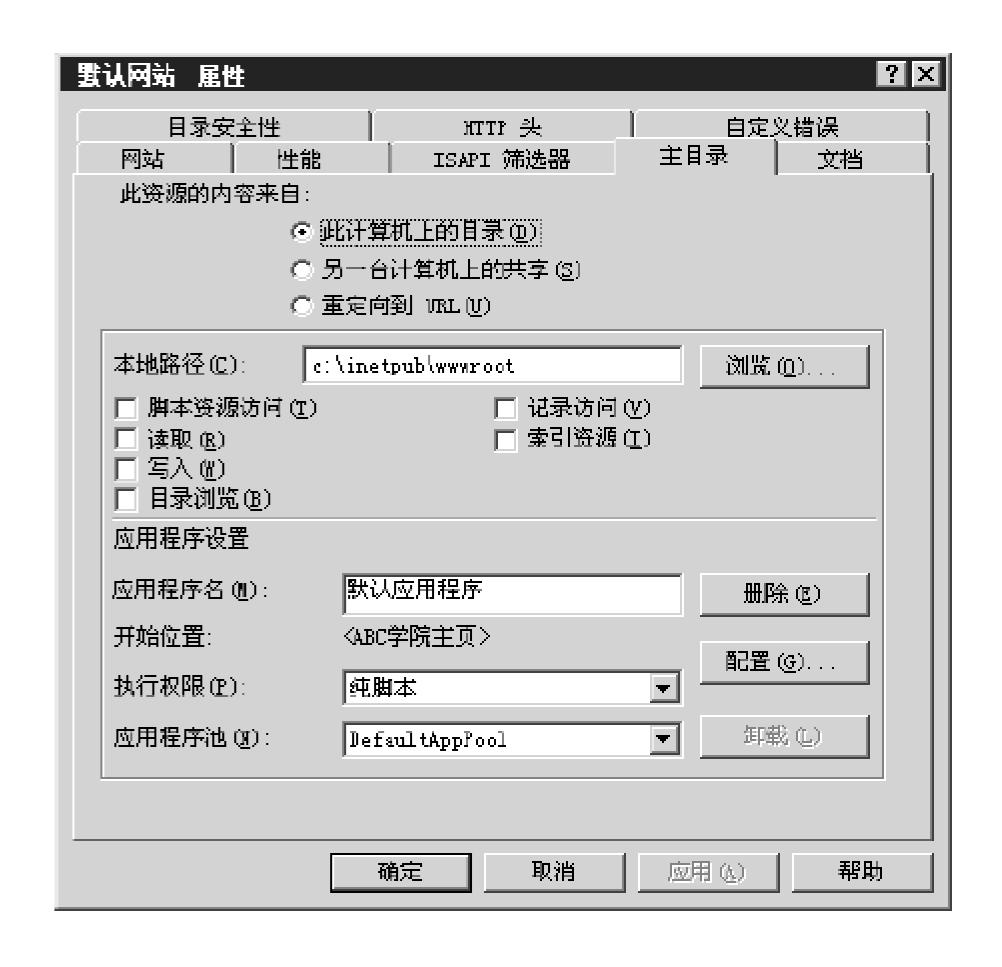



图 8.66　“主目录”选项卡

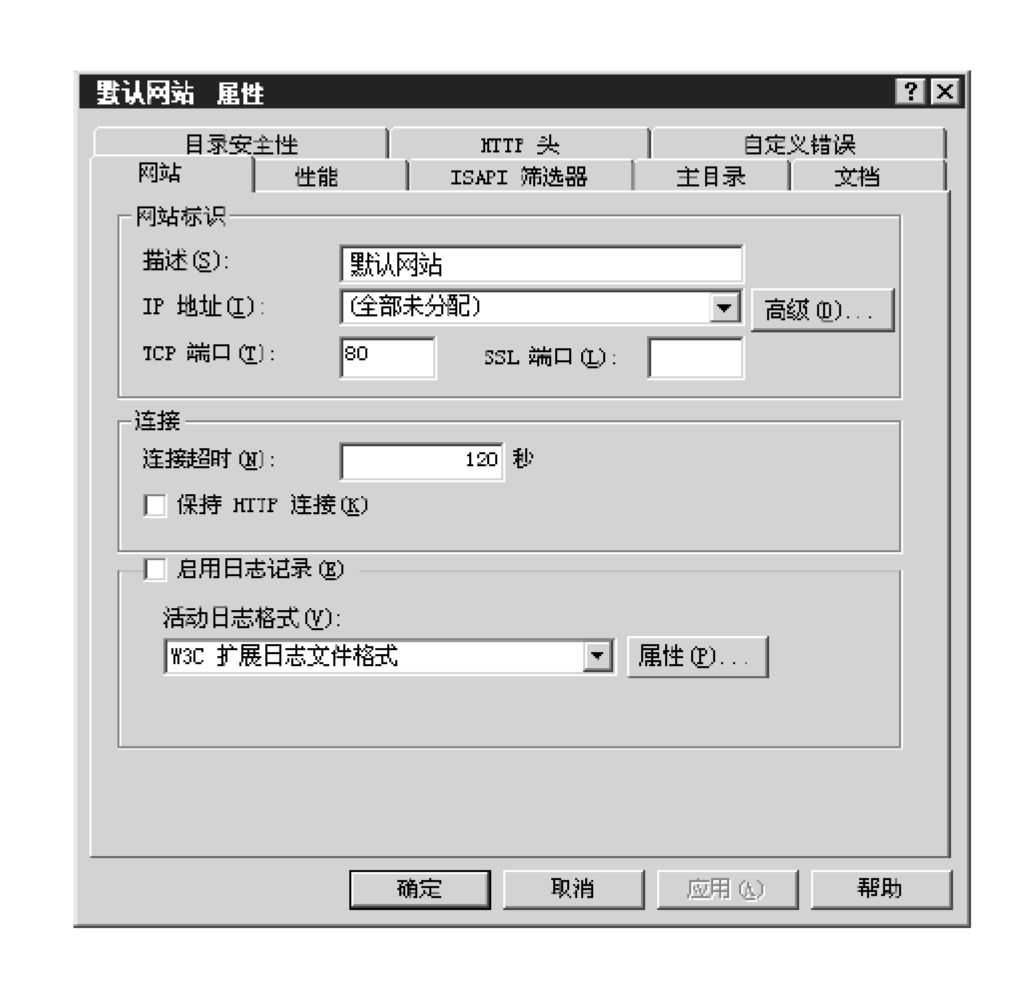


图 8.67　“网站”选项卡

1. 如果要记录用户访问历史，需__(1)__。

(1)备选答案：

A. 同时选中图 8.66 中“写入”复选框和图 8.67 中“启用日志记录”复选框

B. 同时选中图 8.66 中“记录访问”复选框和图 8.67 中“启用日志记录”复选框

C. 同时选中图 8.66 中“记录访问”复选框和“索引资源”复选框

D. 同时选中图 8.66 中“记录访问”复选框和图 8.67 中“保持 HTTP 连接”复选框

2. 在图 8.67 所示的 4 种活动日志格式中，需要提供用户名和密码的是__(2)__。

【问题 2】(4 分)

根据图 8.66 判断正误。(正确的答“对”，错误的答“错”)

A. 选中“读取”是指禁止客户下载网页文件及其他文件。__(3)__

B. 不选中“写入”是指禁止客户以 HTTP 方式向服务器写入信息。__(4)__

C. 选中“目录浏览”是指当客户请求的文件不存在时，将显示服务器上的文件列表。__(5)__

D. 当网页文件是 CGI 文件时，“执行权限”中选择“纯脚本”。__(6)__

【问题 3】(6 分)

FTP 的配置如图 8.68 所示。

匿名用户的权限与在“本地用户和组”的权限__(7)__，FTP 可以设置__(8)__虚拟目录。FTP 服务器可以通过__(9)__访问。

(9)备选答案：

A. DOS、客户端方式　　　　B. 客户端、浏览器方式

C. DOS、浏览器、客户端方式

【问题 4】(6 分)

邮件服务器的配置如图 8.69 所示。

若图 8.69 所示 waws.net 域已经在 Internet 上注册，那么在 DNS 服务器中应配置邮件服务器的__(10)__记录。POP3 是__(11)__邮件协议，配置 POP3 服务器的步骤包含__(12)__(多选)。



图 8.68 “安全账户”选项卡

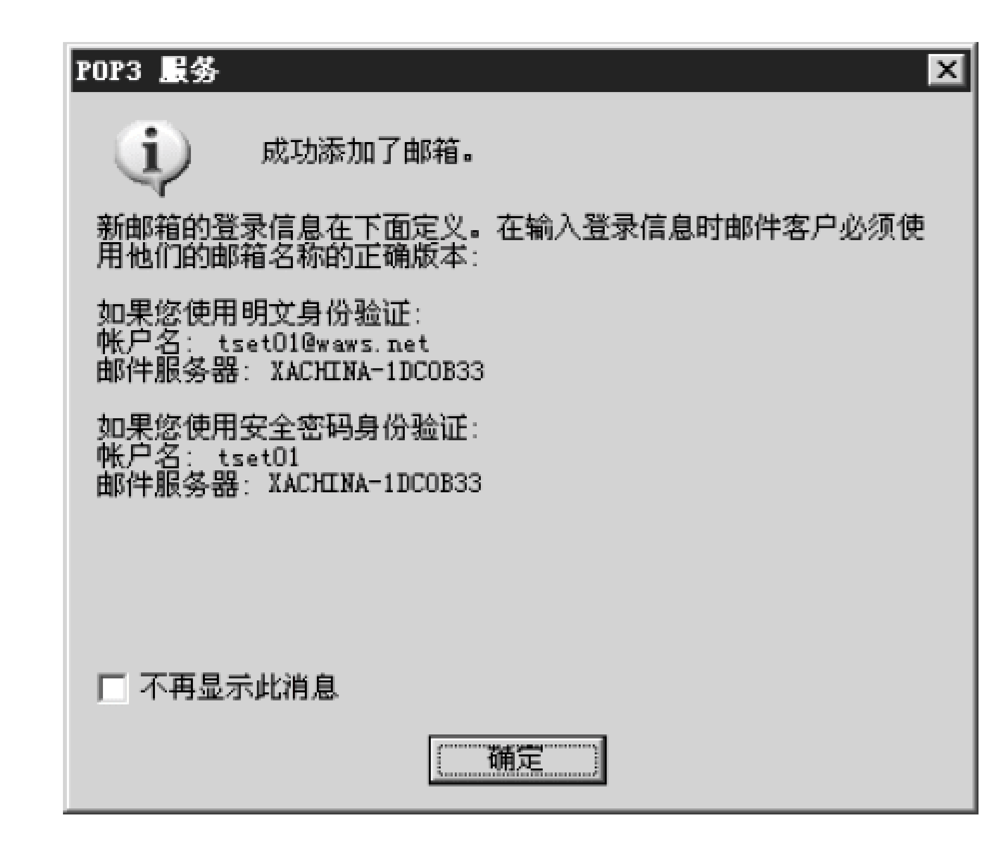


图 8.69 “POP3 服务”对话框

(11)备选答案：

A. 接收　　B. 发送　　C. 存储　　D. 转发

(12)备选答案：

A. 创建邮件域　　B. 设置服务器最大连接数

C. 安装 POP3 组件　　D. 添加邮箱参考答案：

【问题 1】(1)B；(2)ODBC 日志记录。

【问题 2】(3)错；(4)对；(5)对；(6)错。

【问题 3】(7)相同；(8)站点；(9)C。

【问题 4】(10)MX；(11)A；(12)C、A、D。

要点解析：

【问题 1】

记录访问：在日志文件中记录对网站的访问。需要选中“记录访问”和“启用日志记录”复选框。

在 4 种活动日志格式中，只有 ODBC 日志记录需要连接数据库，需要提供用户名和密码。

【问题 2】

读取：由于网站主要是供用户浏览的，一般指需要选择“读取”即可。

写入：客户以 HTTP 方式向服务器写入内容。

目录浏览：客户可以查看服务器上文件的目录结构。

CGI 是外部应用程序(CGI 程序)与 Web 服务器之间的接口标准。当网页是 CGI 时候，执行选项改成脚本和可执行程序。

【问题 3】

匿名用户的权限和“本地用户和组”的权限相同，FTP 设置站点虚拟目录。FTP 服务器可以通过 DOS、浏览器、客户端方式访问。

【问题 4】

MX 记录是用于电子邮件系统发邮件时根据收信人的地址后缀来定位邮件服务器。例如，当收件人为“user@csai.com”时，系统将对“csai.com”进行 DNS 中的 MX 记录解析。如果 MX 记录存在，系统就根据 MX 记录的优先级，将邮件转发到与该 MX 相应的邮件服



务器上。

POP3 是电子邮件接收协议，配置 POP3 服务器的步骤包括安装 POP 组件、创建邮件域、添加邮箱。

试题 6 （2015 年上半年下午试题三）

【说明】

某企业采用 Windows Server 2003 配置了共享打印、FTP 和 DHCP 服务。

【问题 1】(8 分)

1. Internet 共享打印使用的协议是__(1)__。(1 分)

(1)备选答案：

A. PPI　　B. IPP　　C. TCP　　D. IP

2. Internet 共享打印配置完成后，需在如图 8.70 所示的 Web 服务扩展选项卡中将 Active Server Pages 设置为“允许”，其目的是__(2)__。(2 分)

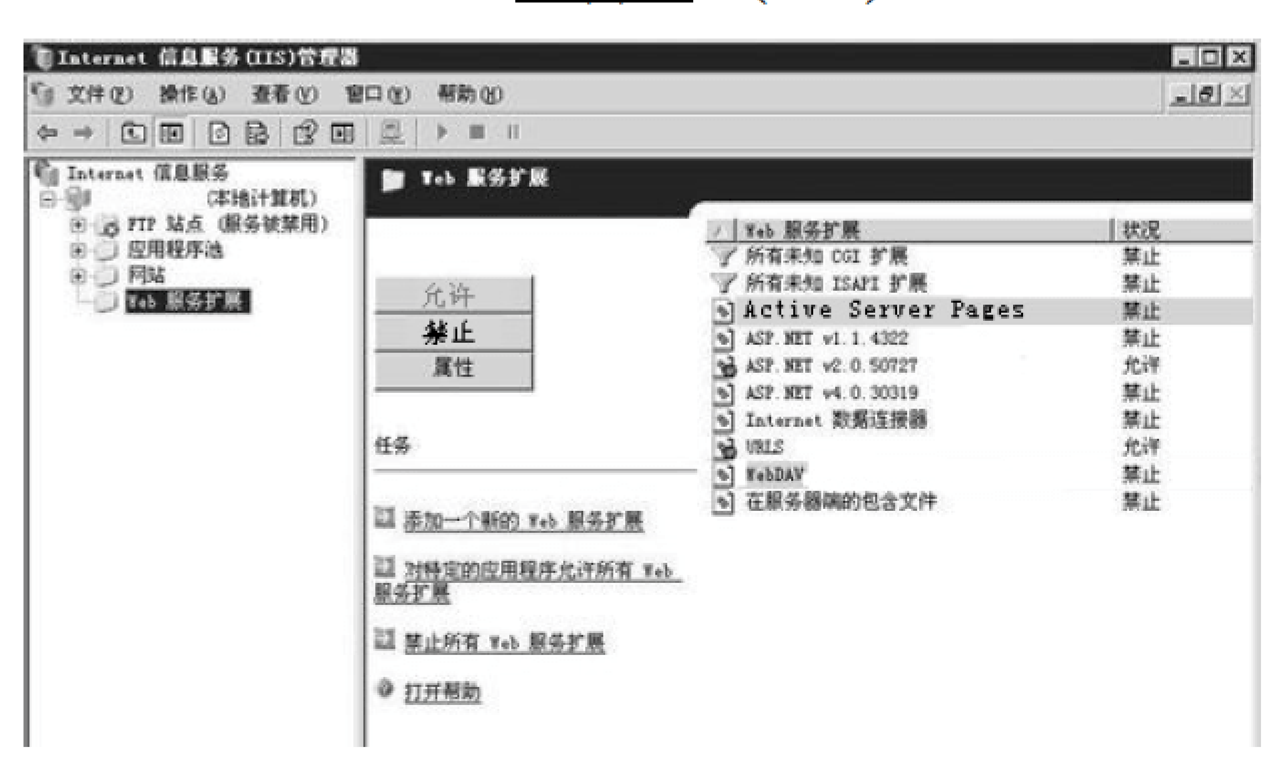


图 8.70　“Web 服务扩展”选项卡

3. 检验 Internet 打印服务是否安装正确的方法是在 Web 浏览器的地址栏输入 URL 是__(3)__。(2 分)

(3)备选答案：

A. HTTP: //127.0.0.1/PRINTERS　　B. FTP: //127.0.0.1/PRINTERS

C. HTTP: //PRINTERS　　D. FTP: //PRINTERS

4. 使用 Internet 共享打印流程为 6 个步骤：

① 在终端上输入打印设备的 URL

② 服务器向用户显示打印机状态信息

③ 客户端向打印服务器发送身份验证信息

④ 用户把要打印的文件发送到打印服务器

⑤ 打印服务器生成一个 cabinet 文件，下载到客户端

⑥ 通过 Internet 把 HTTP 请求发送到打印服务器

对以上步骤进行正确的排序__(4)__。(3 分)

【问题 2】(8 分)

FTP 的配置如图 8.71、图 8.72 所示。



图 8.71 “目录安全性”选项卡

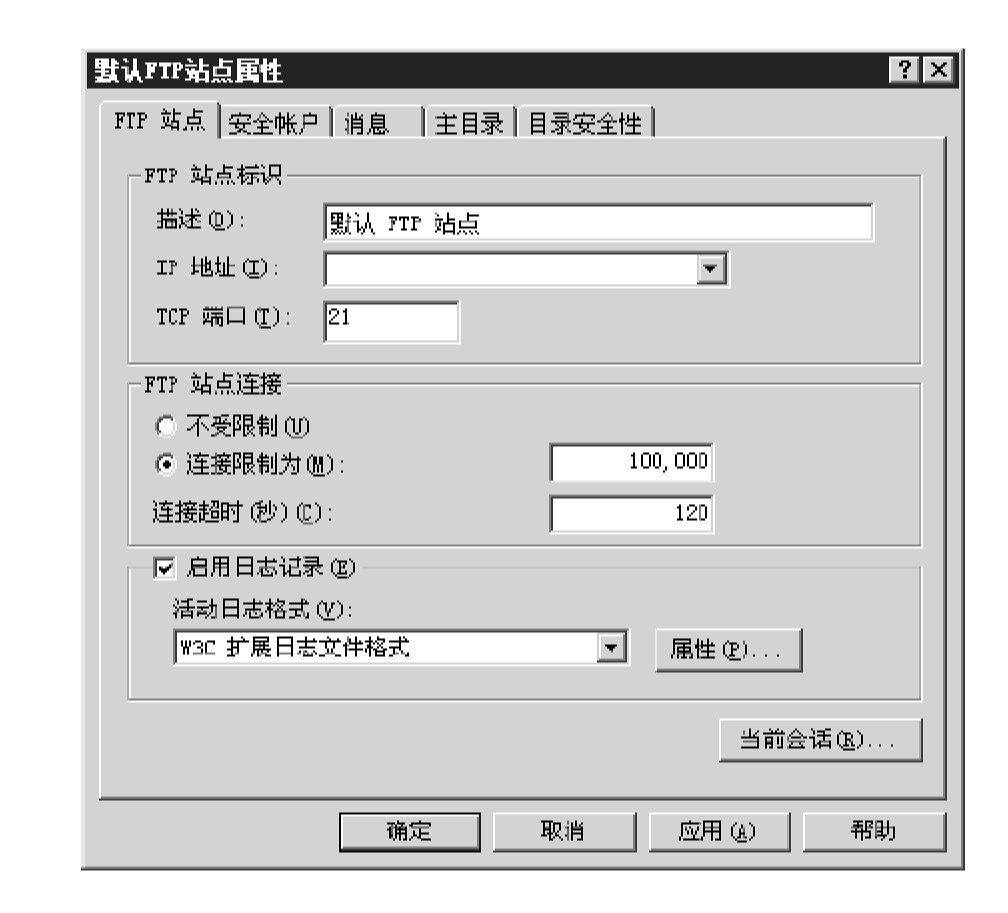


图 8.72 “FTP 站点”选项卡

1. 默认情况下，用户登录 FTP 服务器时，服务器端建立的 TCP 端口号为__(5)__。
2. 如果只允许一台主机访问 FTP 服务器，参考图 8.72 给出具体的操作步骤__(6)__。
3. 参考图 8.72，在一台服务器上搭建多个 FTP 站点的方法是__(7)__。
4. 如单击图 8.72 中“当前会话”按钮，显示的信息是__(8)__。

【问题 3】(4 分)

DHCP 的配置如图 8.73 和图 8.74 所示。



图 8.73 “常规”选项卡

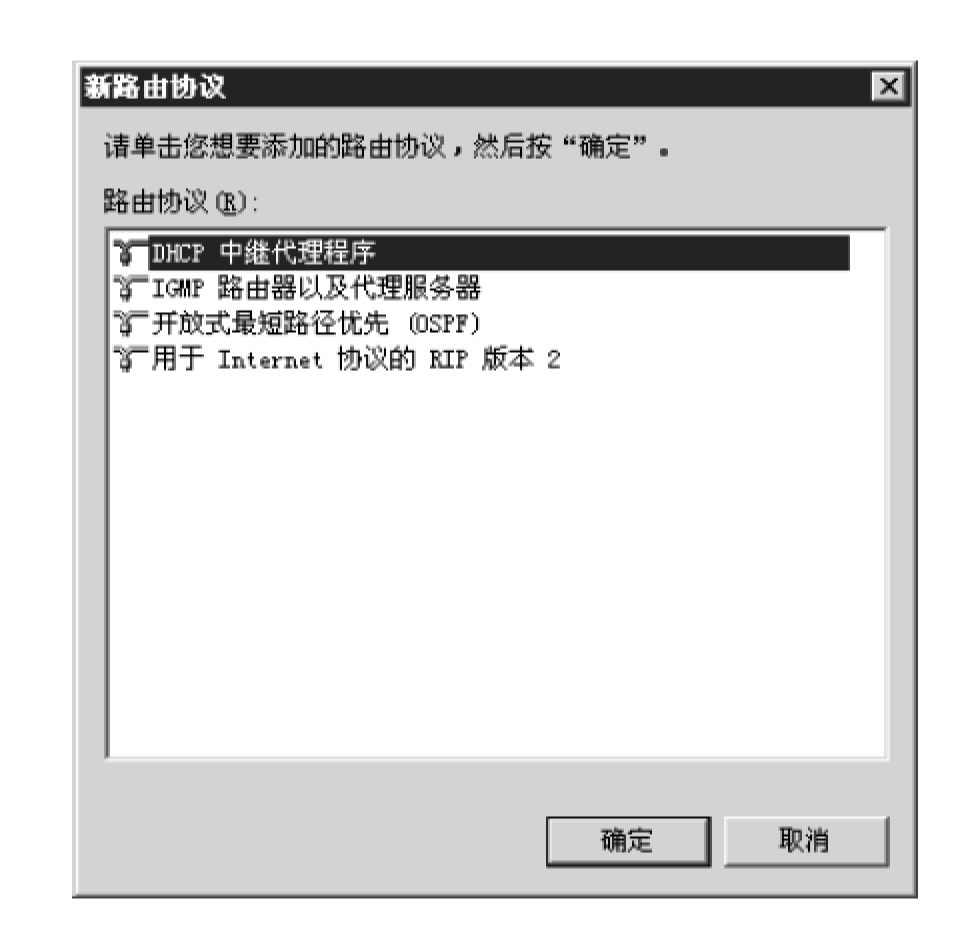


图 8.74 “新路由协议”对话框

1. 图 8.73 中填入的 IP 地址是__(9)__。
2. 图 8.74 中配置 DHCP 中继代理程序，可以实现__(10)__。

(9)备选答案：

A. 分配给客户端的 IP 地址

B. 默认网关的 IP 地址

C. DHCP 服务器的 IP 地址

(10)备选答案：

A. 使普通客户机获取 IP 等信息





B. 跨网段的地址分配

C. 特定用户组访问特定网络

参考答案：

【问题 1】

(1)B；

(2)允许运行 Internet 打印服务的 ASP 脚本；

(3)A；

(4)①⑥③②⑤④。

【问题 2】

(5)21；

(6)选中“拒绝访问”，添加允许计算机的 IP 地址；

(7)不同的 IP 地址或相同的 IP、不同的 TCP 端口；

(8)连接的客户端会话信息。

【问题 3】

(9)B；

(10)B。

要点解析：

【问题 1】

IPP(Internet 打印协议)侦听服务提供了一个 IPP 网络协议服务，该服务为打印客户机系统提供一种与运行侦听程序的系统上的打印服务进行交互的方法。此侦听程序实现了服务器端 IPP 协议支持，其中包括一组广泛的标准操作和属性。

开启 Active Server Pages 服务扩展，以便允许服务器运行 Internet 打印服务的 ASP 脚本文件。

通过 Web 访问 Internet 打印服务器的方法为：HTTP: //127.0.0.1/PRINTERS。

Internet 打印流程如下。

(1) 用户输入打印设备的 URL(统一资源定位符) ，通过 Internet 连接到打印服务器。

(2) HTTP 请求通过 Internet 发送到打印服务器。

(3) 打印服务器要求客户端提供身份验证信息。这样能够确保只有经过授权的用户才能在打印服务器上打印文件。

(4) 当用户获得授权可以访问打印服务器后，服务器使用活动服务器页(Active Server Pages，ASP)向用户显示状态信息，其中包括有关当前空闲打印机的信息。

(5) 当用户连接 Internet 打印网页上的任何打印机时，客户端计算机首先尝试在本地寻找该打印机的驱动程序。如果没有找到适合的驱动程序，打印服务器将会生成一个 cabinet 文件(.cab 文件，又称为 Setup 文件)，其中包含正确的打印机驱动程序文件。打印服务器把 .cab 文件下载到客户端计算机上。客户端计算机提示用户允许下载该.cab 文件。

(6) 当用户连接到 Internet 打印机后，他们可以使用 Internet 打印协议 (Internet Printing Protocol，IPP)把文件发送到打印服务器。

【问题 2】

FTP 使用的 TCP 端口号为 21。

“目录安全性”选项卡中，只允许单台主机访问，可以选中“拒绝所有”，然后添加主机的 IP 地址。

搭建多个 FTP 站点的方式是：不同 IP 地址或相同的 IP、不同的端口号。

“当前会话”中，显示了连接到 FTP 服务器的客户端信息。

【问题 3】

配置 DHCP 服务器选项时，003 路由器设置分配给客户端的网关地址。通过 DHCP 中继代理，可以实现跨网段的地址分配。

8.4 强化训练

8.4.1 综合知识试题

试题 1 (2014 年下半年试题 31)

管理员为某台 Linux 系统中的/etc/hosts 文件添加了如下记录，下列说法中正确的是 (31) 。

127.0.0.1 localhost.localdomain localhost

192.168.1.100 linumu100.com web80

192.168.1.120 emailserver

(31) A. linumu100.com 是主机 192.168.1.100 的主机名

B. web80 是主机 192.168.1.100 的主机名

C. emailserver 是主机 192.165.1.120 的别名

D. 192.168.1.120 行记录的格式是错误的

试题 2 (2014 年下半年试题 32)

下列关于 Linux 文件组织方式的说法中， (32) 是错误的。

(32) A. Linux 文件系统使用索引节点来记录文件信息

B. 文件索引节点号由管理员手工分配

C. 每个文件与唯一的索引节点号对应

D. 一个索引节点号可对应多个文件

试题 3 (2014 年下半年试题 35)

在 Windows 系统中可通过停止 (35) 服务器来阻止对域名解析 Cache 的访问。

(35) A. DNS Server　B. Remote Procedure　C. Ns lookup　D. DNS Client

试题 4 (2014 年下半年试题 38)

在 Linux 操作系统中，采用 (38) 来搭建 DNS 服务器。

(38) A. Samble　B. Tomcat　C. Bind　D. Apache





试题 5 (2014 年下半年试题 40)

使用__(40)__命令可以向 FTP 服务器上传文件。

(40) A. get　B. dir　C. put　D. push

试题 6 (2014 年下半年试题 49)

以下关于 Windows Server 2003 域管理模式的描述中，正确的是__(49)__。

(49) A. 域间信任关系只能是单向信任
B. 单域模型中只有一个主域控制器，其他都为备份域控制器
C. 如果域控制器改变目录信息，应把变化的信息复制到其他域控制器
D. 只有一个域控制器可以改变目录信息

试题 7 (2014 年上半年试题 31)

在 Linux 系统的服务器中，使用 BIND 配置域名服务，主配置文件存放在__(31)__中。

(31) A. name.conf　B. named.conf　C. dns.conf　D. dnsd.conf

试题 8 (2014 年上半年试题 32)

在运行 Linux 系统中，root 用户执行 shutdown-r now 命令，系统将会__(32)__。

(32) A. 重新启动　B. 进入单用户模式　C. 休眠　D. 关机

试题 9 (2014 年上半年试题 46)

在 Windows Server 2003 环境中有本地用户和区域用户两种，其中本地用户信息存储在__(46)__。

(46) A. 本地计算机的 SAM 数据库　B. 本地计算机的活动目录
C. 域控制器的活动目录　D. 域控制器的 SAM 数据库

8.4.2 案例分析试题

试题 1 (2014 年下半年下午试题二)

【说明】

某中学为两个学生课外兴趣小组提供了建立网站的软硬件环境。网站环境的基本配置方案如下。

1. 两个网站配置在同一台服务器上，网站服务由 Windows Server 2003 环境下的 IIS 6.0 提供。

2. 网站的管理通过 Windows Server 2003 的远程桌面实现，并启用 Windows Server 2003 的防火墙组件。

3. 为兴趣小组建立各自独立的文件夹作为上传目录和网站的主目录，对用户使用磁盘空间大小进行了设定。

4. 通过不同的域名分别访问课外兴趣小组各自的网站。

按照方案，学校的网络工程师安装了 Windows Server 2003 服务器，使用 IIS 6.0 建立 Web 和 FTP 服务器，配置了远程桌面管理、防火墙，在服务器上为两个课外兴趣小组分配了不同的用户名，进行了初步的权限配置。

【问题 1】(4 分)

Windows 2003 远程桌面服务的默认端口是__(1)__，对外提供服务使用__(2)__协议。在图 8.75 中，若要拒绝外部设备 ping 服务器，在防火墙的 ICMP 配置界面上应该如何操作？

【问题 2】(4 分)

1. 在图 8.76 中，“Web 服务扩展”选项中“所有未知 CGI 扩展禁止”的含义是什么？
2. 在图 8.76 中，如何配置 Web 服务扩展，网站才能提供对 asp.net 或 ASP 程序的支持？

【问题 3】(5 分)

在图 8.76 中，选择 IIS 管理器中的“FTP 站点”→“新建”→“虚拟目录”，分别设置 FTP 用户与__(3)__、__(4)__的对应关系。

由于 IIS 内置的 FTP 服务不支持__(5)__，所以 FTP 用户密码是以明文方式在网络上传输，安全性较弱。

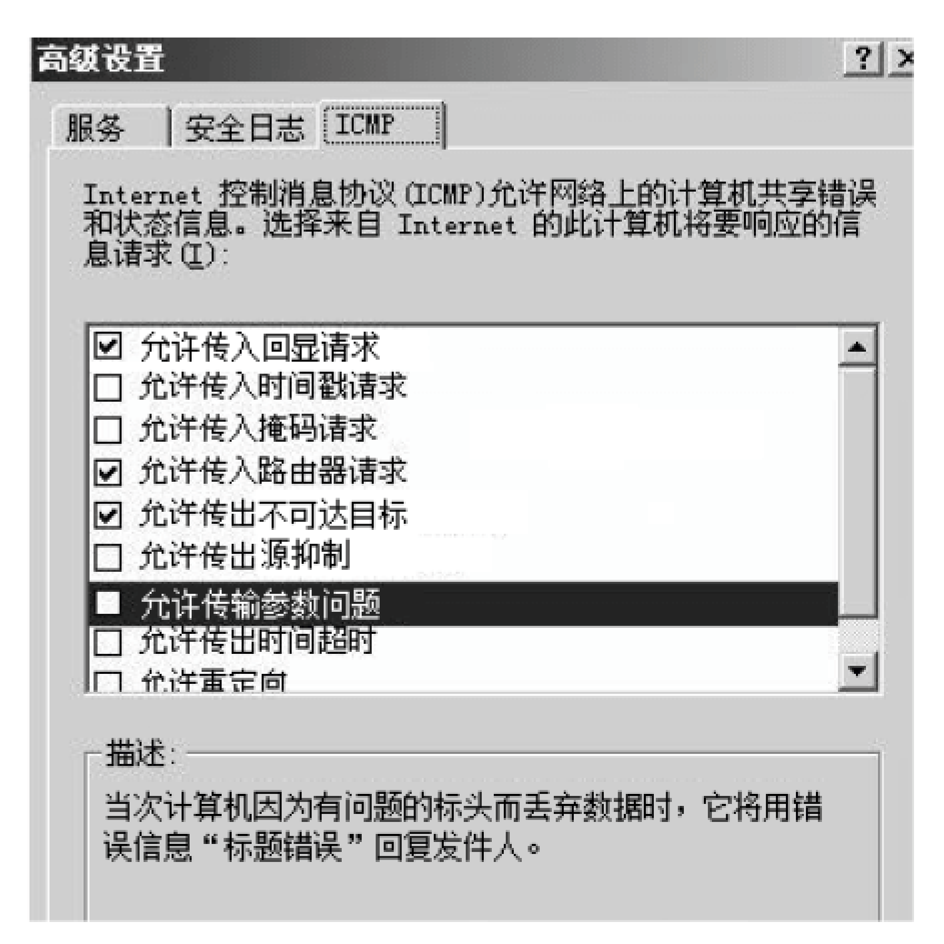


图 8.75 “高级设置”对话框



图 8.76 Web 服务扩展

【问题 4】(4 分)

在 IIS 6.0 中，每个 Web 站点都具有唯一的、由三部分组成的标识符，用来接收和响应请求，分别是__(6)__、__(7)__和__(8)__。网络工程师通过单击“网站属性”→“网站”→“高级选项”通过添加__(9)__的方式在一个 IP 地址上建立多个网站。

【问题 5】(3 分)

在__(10)__文件系统下，为了预防用户无限制地使用磁盘空间可以使用磁盘配额管理。启动磁盘配额时，设置的两个参数分别是__(11)__和__(12)__。

试题 2 (2014 年上半年下午试题二)

【说明】

某公司采用 Windows Server 2003 操作系统搭建该公司的企业网站，要求用户在浏览器地址必须输入 https://www.gqngsi.com/index.html 或 https://117.112.89.67/index.html 来访问该公司的网站。其中，index.html 文件存放在网站服务器 E:\gsdata 目录中。在服务器上安装完成 IIS 6.0 后，网站属性窗口“网站”“主目录”选项卡分别如图 8.77 和图 8.78 所示。




图 8.77　“网站”选项卡



图 8.78　“主目录”选项卡

【问题 1】(4 分)

1. 按照题目说明，图 8.77 中的“IP 地址”下拉列表框中的内容为__(1)__；“SSL 端口”文本框内容为__(2)__。

2. 在图 8.78 中，“本地路径”文本框中的内容为__(3)__；同时要保障用户通过题目要求的方式来访问网址，必须至少选中__(4)__复选框。

(4)备选答案：

A. 脚本资源访问　　B. 读取

C. 写入　　D. 目录浏览

【问题 2】(6 分)

1. 配置该网站时，要在如图 8.75 所示“目录安全性”选项卡中单击“服务器证书”按钮来获取服务器证书，其中获取服务器证书的步骤顺序如下：①生产证书请求文件；②__(5)__；③从 CA 导出证书文件；④在 IIS 服务器上导入安装文件。

配置完成后，当用户登录该网站时，通过验证 CA 的签名来确认数字证书的有效性，从而__(6)__，CA 颁发给 Web 网站的数字证书不包括__(7)__。

(6)、(7)备选答案：

(6) A. 验证网站的真伪　　B. 判断用户的权限

C. 加密发送服务器的数据　　D. 解密所接收的客户端数据

(7) A. 证书的有效期　　B. 网站的公钥

C. 证书的序列号　　D. 网站的私钥

【问题 3】(2 分)

配置该网站时，在图 8.79 的窗口中单击“安全通信”选项组中的“编辑”按钮，弹出如图 8.80 所示对话框，按题目要求，客户端浏览器只能通过 HTTPS 方式访问服务器，此时应选中图 8.80 中的__(8)__框，如果要求客户端和服务器进行双向认证，此时应选中图 8.80 中的__(9)__框。

【问题 4】(2 分)

HTTPS 用于在客户计算机和服务器之间提供安全通信，广泛用于因特网上安全敏感的应用，例如__(10)__应用。

HTTPS 使用安全套接子层(SSL)进行信息交换。SSL 目前版本是 3.0，被 IETF 定义在 RFC 6101 中。IETF 对 SSL 进行升级后的继任者是__(11)__。

(10) 备选答案：

A. 网络聊天　　B. 网络视频　　C. 网上交易　　D. 网络下载

【问题 5】(1 分)

使用 HTTPS 能不能确保服务器自身安全？



图 8.79　“目录安全性”选项卡



图 8.80　“安全通道”对话框

试题 3 (2014 年上半年下午试题三)

【说明】

某单位网络拓扑结构如图 8.81 所示，在 Linux 系统下构建 DNS 服务器、DHCP 服务器和 Web 服务器，要求如下。

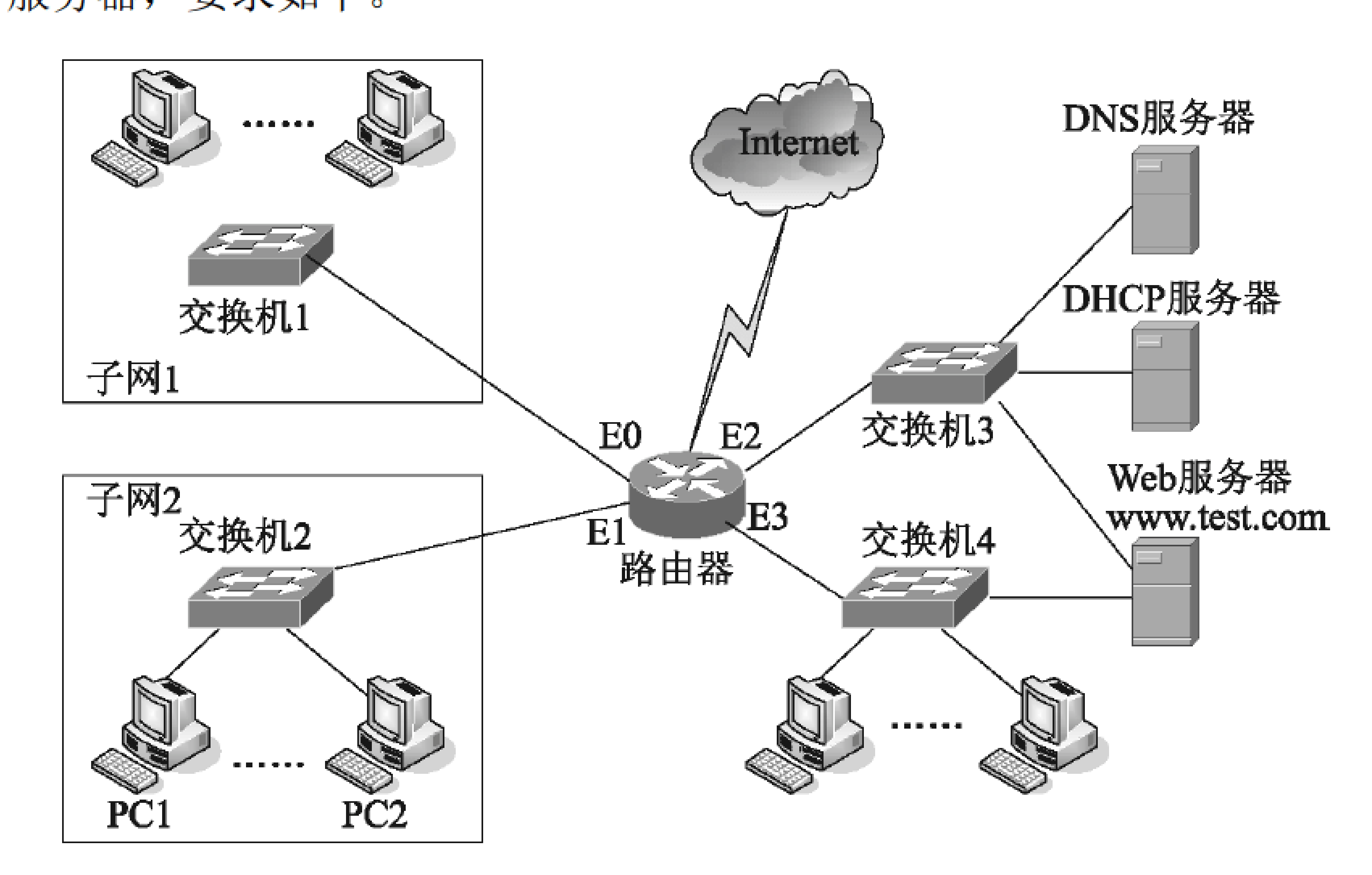


图 8.81　网络拓扑结构图

1. 路由器连接各个子网的接口信息如下：

(1)　路由器 E0 的 IP 地址 192.168.1.1/25。

(2)　路由器 E1 的 IP 地址 192.168.1.129/25。



(3) 路由器 E2 的 IP 地址 192.168.2.1/25。
(4) 路由器 E3 的 IP 地址 192.168.2.33/25。
2. 子网 1 和子网 2 内的客户机通过 DHCP 服务器动态分配 IP 地址。
3. 服务器设置固定的 IP 地址，其中：
(1) DNS 服务器采用 BIND 构建，IP 地址为 192.168.2.2。
(2) DHCP 服务器 IP 地址为 192.168.2.3。
(3) Web 服务器网卡 eth0 的 IP 地址为 92.168.2.4，eth1 的 IP 地址为 92.168.2.34。

【问题 1】(3 分)

请完成图 8.81 中 Web 服务器 eth1 的配置。

```
Device=eth1
Bootproto=static
Onboot=yes
Hwaddr=08:00:27:24:F8:9B
Netmask= (1)
Ipaddr= (2)
Gateway= (3)
Type=Ethernet
Name="Systemeth1"
Ipv6intt=no
```

【问题 2】

请完成 DNS 服务器上的配置。

```
Device=eth0
Bootproto=static
Onboot=yes
Hwaddr=08:00:27:21:A1:78
Netmask= (4)
Ipaddr= (5)
Gateway= (6)
Type=Ethernet
Name="Systemeth0"
Ipv6intt=no
```

【问题 3】

在(7)、(8)、(9)处填写恰当的内容。在 Linux 系统中设置域名解析服务器，已知域名服务器上文件 named.conf 的部分内容如下：

```
options{
Directory "/var/named";
Hostname "nsl.test.com";
allow-query {any;};
allow-recursion {A:B:C:D};
Recursion yes;
};
acl "A" {192.168.1.0/25};
acl "B" {192.168.1.128/25};
acl "C" {192.168.2.0/29};
```



```
acl "D"{192.168.1.32/29};
View "A"{
Match-clients{A;};
Recursion yes;
Zone "test.com"{
Type master;
File "test.com.zone.A"
};
};
View "B"{
Match-clients{any;};
Recursion yes;
Zone "test.com"{
Type master;
File "test.com.zone.B"
};
};
```

test.com.zone.A 文件的部分配置如下：WWW IN A 192.168.2.4。

test.com.zone.B 文件的部分配置如下：WWW IN B 192.168.2.34。

IP 地址__(7)__不允许使用该 DNS 进行递归查询，子网 1 和子网 2 中的客户端访问 www.test.com 时，该 DNS 解析返回的 IP 地址分别为__(8)__和__(9)__。

(7)备选答案：

A. 192.168.1.8　　B. 192.168.2.34

C. 192.168.2.10　　D. 192.168.2.6

(8)、(9)备选答案：

A. 192.168.2.4　　B. 192.168.2.34

C. 192.168.2.4 或者 192.168.2.34　　D. 192.168.2.4 和 192.168.2.34

【问题 4】

DHCP 服务器配置文件如下：

```
Authoritative;
Ddns-update off;
Max-lease-time 604800;
default-lease-time 604800;
Allow unknow-clients;
Option domain-name-servers 192.168.2.2;
Ddns-update-style none;
allow client-update;
subnet 192.168.0.0 netmask 255.255.255.248{
option routers 192.168.2.33;
range 192.168.2.35 192.168.2.38;
}
```

根据这个文件内容，该 DHCP 服务器默认租期__(10)__天。DHCP 客户机能获得的 IP 地址范围是从__(11)__到__(12)__，获得 DNS 服务器 IP 地址为__(13)__。

8.4.3　综合知识试题参考答案

【试题 1】答　案：(31)A。

解　析：hosts 文件是 Linux 系统上一个负责 IP 地址与域名快速解析的文件，以 ASCII 格式保存在/etc/目录下。hosts 文件包含了 IP 地址与主机名之间的映射，还包括主机的别名。在没有域名解析服务器的情况下，系统上的所有网络程序都通过查询该文件来解析对应于某个主机名的 IP 地址，否则就需要使用 DNS 服务程序来解决。通过可以将常用的域名和 IP 地址映射加入 hosts 文件中。hosts 文件格式如下：

```
IP 地址    主机名/域名    (主机别名)
```

web80 是主机 192.168.1.100 的别名，emailserver 是主机 192.165.1.120 的主机名。

【试题 2】答　案：(32)B。

解　析：Linux 为每个文件分配一个称为索引节点的编号，可以将索引节点简单理解成一个指针，它永远指向本文件在物理磁盘上的具体存储位置。系统是通过索引节点(而不是文件名)来定位每一个文件的。

【试题 3】答　案：(35)D。

解　析：DNS 分为 Client 和 Server，Client 扮演发问的角色，也就是问 Server 一个 Domain Name，而 Server 必须回答此 Domain Name 的真正 IP 地址。而当地的 DNS 先会查自己的资料库。如果自己的资料库没有，则会往该 DNS 上所设的 DNS 服务器询问，依此得到答案之后，将收到的答案存起来，并回答客户。DNS 服务器会根据不同的授权区(Zone)，记录所属该网域下的各名称资料，这个资料包括网域下的次网域名称及主机名称。在每一个名称服务器中都有一个快取缓存区(Cache)，这个快取缓存区的主要目的是将该名称服务器所查询出来的名称及相对的 IP 地址记录下来，这样当下一次还有另外一个客户端到此服务器上去查询相同的名称时，服务器就不用再到别的主机上去寻找，而直接可以从缓存区中找到该笔名称记录资料，传回给客户端，加速客户端对名称查询的速度。

【试题 4】答　案：(38)C。

解　析：在 Linux 操作系统中，通过安装 Bind 软件包，来搭建 DNS 服务器。Bind 是一个客户机/服务器系统，客户端称为转换程序，负责查询产生域名的信息，再将这些信息发送给服务器。服务器端称为 named 守护进程，负责查询转换程序。

【试题 5】答　案：(40)C。

解　析：get 命令——使用当前文件转换类型将远程文件复制到本地计算机。

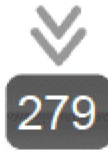
dir 命令——显示远程目录文件和子目录列表。

put 命令——使用当前文件传送类型将本地文件复制到远程计算机上。

【试题 6】答　案：(49)C。

解　析：域间的信任关系可以是单向信任，也可以是双向信任。Windows 2003 域中采用多主模式，每一台域控制器的地位是相同的，域控制改变目录信息，将会有所变化的信息复制到其他域控制器里，并且每一台域控制器都可以改变目录信息。

Windows Server 2003 的活动目录是由组织单元(OU)、域(domain)、域树(tree)、森林(forest)构成的层次结构。活动目录为每个域建立一个目录数据库的副本，这个副本只存储用于这个域的对象。如果多个域之间有相互关系，它们可以构成一个域树。在每个域树中，每个



域都拥有自己的目录数据库副本来存储自己的对象，并且可以查找域树中其他目录数据库的副本。多个域树构成了森林。

活动目录提供域间的信任关系及跨域的安全。当域之间有信任关系时，每个域的认证机构都信任其他所有它信任的域的认证机构。如果一个 user 或 application 被一个域认证以后，所有信任这个认证域的域都认同这种模式。一个被信任域中的用户都必须受到信任域上的访问控制。

【试题7】答　案：(31)B。

解　析：DNS 即 Domain Name System 的缩写，是一种将 IP 地址转换成对应的主机名或将主机名转换成与之相对应 IP 地址的一种机制。BIND 是 Linux 平台下配置 DNS 服务的主程序，可以使用 RPM 或编译安装软件，之后会在 Linux 主机上形成一个/etc/named.conf 文件，该文件是作为 Linux 平台 DNS 服务的配置文件。

【试题8】答　案：(32)A。

解　析：Linux 系统中采用 shutdown -rnow 命令重新启动系统。

shutdown 常用命令参数：

-t seconds：设定在几秒钟之后进行关机程序；

-k：并不会真的关机，只是将警告信息传送给所有使用者；

-r：关机后重新开机；

-h：关机后停机；

-n：不采用正常程序来关机，用强迫的方式杀掉所有执行中的程序后自行关机；

-c：取消目前已经进行中的关机动作；

-f：关机时，不做 fsck 动作(检查 Linux 档系统)；

-F：关机时，强迫进行 fsck 动作；

time：设定关机的时间；

message：传送给所有使用者的警告信息。

【试题9】答　案：(46)A。

解　析：本地用户账户仅允许用户登录并访问创建该账户的计算机。当创建本地用户账号时，Windows Server 2003 仅在计算机位于%Systemroot%\system32\config 文件夹下的安全数据库(SAM)中创建该账户。

8.4.4　案例分析试题参考答案

试题1　答案与解析

答　案：

【问题1】

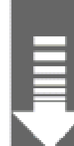
(1)3389；(2)RDP。

去掉勾选“允许传入回显请求”。

【问题2】

1. 除非明确允许一个应用在 IIS 6.0 上允许，否则就禁止运行，提高安全性。
2. Active Server Pages 修改为允许。





【问题 3】

(3)xiaozu-a；(4)xiaozu-b；(5)SSL。

【问题 4】

(6)IP 地址；(7)端口；(8)域名；(9)主机头。

【问题 5】

(10)NTFS；(11)磁盘配额限制；(12)磁盘配额警告级别。

解　析：

【问题 1】

本题考查 Windows Server 2003 服务器配置的相关知识。

远程桌面是方便 Windows 服务器管理员对服务器进行基于图形界面的远程管理的工具。远程桌面是基于 RDP (Remote Desktop Protocol 远程桌面协议)的多通道 (multi-channel)协议，让使用者(所在计算机称为用户端或"本地计算机")连上提供服务器或"远程计算机"，远程桌面默认使用的端口是 3389。

ICMP 协议是一种用于传输出错报告控制信息，对于网络安全具有极其重要的意义。它是 TCP/IP 协议簇的一个子协议，属于网络层协议，主要用于在主机与路由器之间传递控制信息，包括报告错误、交换受限控制和状态信息等。当遇到 IP 数据无法访问目标，IP 路由器无法按当前的传输速率转发数据包等情况时，会自动发送 ICMP 消息。

【问题 2】

如果选择允许所有通用网关接口(CGI)在 Web 服务器上运行，则 Web 服务器容易受到使用 CGI 技术的计算机病毒或蠕虫程序的攻击。禁止该扩展意味着除非明确地允许一个应用在 IIS 6.0 上运行，否则它就不能运行。

要想网站提供对 ASP.NET 或 ASP 程序的支持，必须增加 ASP.NET 模块(启用 ASP.NET 的服务扩展项)。将 Active Server Pages 配置为"允许"，IIS 6.0 即可提供对 ASP 支持。

【问题 3】

FTP (File Transfer Protocol，FTP)是 TCP/IP 网络上两台计算机传送文件的协议，FTP 是在 TCP/IP 网络和 Internet 上最早使用的协议之一，它属于网络协议的应用层。FTP 客户机可以给服务器发出命令来下载文件、上传文件、创建或改变服务器上的目录，FTP 的默认端口是 21。由于 IIS 中的 FTP 服务不支持安全套接字层(SSL)上的 FTP，因此，如果要保证通信的安全性，同时又需要使用 FTP 作为传输协议(相对于在 SSL 上使用 WebDAV 而言)，可以考虑在加密通道(如虚拟专用网络)上使用 FTP，此类加密通道通过点对点隧道协议或 IPSec 保证安全性。

【问题 4】

IIS 是一种 Web (网页)服务组件，其中包括 Web 服务器、FTP 服务器、NNTP 服务器和 SMTP 服务器，分别用于网页浏览、文件传输、新闻服务和邮件发送等方面。IIS 6.0 增强了安全性，为了尽量减少系统被攻击的危险，在默认情况下 IIS 6.0 是不会被安装在 Windows Server 2003 中的，管理员需要手动进行安装，IIS 6.0 在被锁定状态中只为静态内容(.htm, .jpg, .bmp 等等)提供服务，通过网络服务扩展节点，网站管理员可根据企业的需求启用或禁止 IIS 功能。

【问题 5】

在 NTFS 文件系统下，为了预防用户无限制地使用磁盘空间，可以使用磁盘配额管理。启动磁盘配额时，设置的两个参数分别是磁盘配额限制和磁盘配额警告级别。

试题 2　答案与解析

答　案：

【问题 1】

(1)117.112.89.67；(2)443；(3)E:\gsdata；(4)B。

【问题 2】

(5)提交证书申请；(6)A；(7)D。

【问题 3】

(8)“要求安全通道(SSL)”；(9)“要求客户端证书”。

【问题 4】

(10)C；(11)TLS。

【问题 5】不能。

解　析：

【问题 1】

1. 题干中明确说明可以通过 https://117.112.89.67/index. html 访问公司网站，则在图 8.77 中“网站”选项卡的“IP 地址”文本框输入的 IP 址为 117.112.89.67。

SSL(Secure Sockets Layer，安全连接层)及其继任者安全传输层(Transport Layer Security，TLS)是为网络通信提供安全及数据完整性的一种安全协议。TLS 与 SSL 在传输层对网路连接进行加密。该协议结合 HTTP 构成 HTTPS 协议，HTTPS 协议是 HTTP 的安全升级版，该协议基于 TCP 443 端口。

2. 题干中明确说明 index. html 文件放在网站服务器 E:\gsdata 目录中，图 8.78“本地路径”文本框应填入 E:\gsdata。对于一个网站而言，可以通过 IP 或域名的方式访问，在图 8.78 中至少应该开启“读取”权限，否则此网站是不能访问的。

【问题 2】

为了保证网站与客户交互过程中的安全性，可以为网站服务器向 CA 申请服务器证书，证书上绑定了服务器的 ID 和公钥，用户访问此网站时，下载服务器证书，并利用服务器上的公钥加密交互信息，以达到机密性的要求。服务器向 CA 申请证书的过程为：

① 生成证书请求文件。

② 提交证书申请。

③ 从 CA 导出证书文件。

④ 在 IIS 服务器上导入并安装证书。

用户访问网站服务器时，下载服务器证书首先通过证书上 CA 的签名鉴别该证书的合法性，就好像日常生活中办理宾馆入住要先提交身份证一样。确认该服务器证书合法之后，表示客户端信任了该证书的主体(网站服务器)。X.509 标准规定了证书包含版本、序列号、签名算法标识符、签发人签名、有效期、主体名、主体公钥信息等，但不包含证书主体的私钥。

【问题 3】

客户端只能通过 HTTPS 方式访问网站服务器，则应该开启 SSL 功能，通过选中图 8.80

中“要求安全通道(SSL)”复选框开启。客户端可以以 HTTPS 方式访问网站，而且可以下载服务器证书，验证证书合法性以及利用服务器证书公钥加密信息。若服务器和客户端要进行双向认证，亦即客户端验证服务器证书的合法性同时服务器也要验证客户端证书的合法性，以实现双向信任。要在客户端安装客户端证书而且在网站服务器图 8.80 界面上选中“要求客户端证书”单选按钮。

【问题 4】

HTTPS(Hypertext Transfer Protocol over Secure Socket Layer)是以安全为目标的 HTTP 通道，简单讲是 HTTP 的安全版，即 HTTP 下加入 SSL 层。

HTTPS 的安全基础是 SSL，因此加密的详细内容就是 SSL。它是一个 URI scheme(抽象标识符体系)，句法类同 HTTP 体系，用于安全的 HTTP 数据传输。

https://URL 表明它使用了 HTTP，但 HTTPS 存在不同于 HTTP 的默认端口及一个加密/身份验证层(在 HTTP 与 TCP 之间)。这个系统的最初研发由网景公司进行，提供了身份验证与加密通信方法，现在它被广泛用于万维网上安全敏感的通信，例如网上交易支付方面。

在问题 1 的解析文字中已经说明 TLS 为 SSL 的后继版本。

【问题 5】

HTTPS 只是负责用户服务器和客户机交互时的合法性验证以及交互信息的安全，但不能保证服务器自身的安全，比如黑客攻击、DOS 攻击，这些防范是 HTTPS 做不到的。

试题 3　答案与解析

答　案：

【问题 1】

(1)255.255.255.248；(2)192.168.2.34；(3)192.168.2.33。

【问题 2】

(4)255.255.255.248；(5)192.168.2.2；(6)192.168.2.1。

【问题 3】

(7)C；(8)A；(9)B。

【问题 4】

(10)7；(11)192.168.2.35；(12)192.168.2.38；(13)192.168.2.2。

解　析：

【问题 1】

题干已经说明 Web 服务器的 eth1 接口 IP 地址为 192.168.2.34，由于该接口与路由器 E3 接口属于一个逻辑网路，所以其子网掩码长度为“/29”，十进制的表示为 255.255.255.248，路由器 E3 接口 IP 地址 192.168.2.33/29 为 Web 服务器 eth1 接口的网关地址。

【问题 2】

与问题 1 的分析类似，DNS 服务器网卡(eth0)接口 IP 地址为 192.168.2.2，网关为路由器 E2 接口 IP 地址 192.168.2.1/29 的子网掩码长度为 255.255.255.248。

【问题 3】

本问题考查 Linux 系统下基于 BIND 的 DNS 服务配置。

通过 allow-recursion{A;B;C;D}命令，可以看出 acl A、B、C、D 允许递归查询，选项 A、B、D 对应的 IP 地址分别在定义的 acl A、B、C 子网中，选项 C 对应的 IP 地址不在 acl A、

B、C、D 任何子网中，故选 C。

客户端访问 www.test.com 时，子网 1 的客户端对应 ac1A，会访问 view A 中的域名配置文件 test.com.zone.A，故解析出的 IP 地址为 192.168.2.4；子网 2 的客户端不在 acl A 中，则会访问 view B 中的域名配置文件 test.com.zone.B，故解析出的 IP 地址为 192.168.2.34。

【问题 4】

通过 DHCP 服务器配置命令中“default-lease-time 604800”语句分析，默认租约时间为 604800 秒，亦即 7 天。通过语句“option domain-name-servers 192.168.2.2”，可以得到 DHCP 服务器获得的 DNS IP 地址为 192.168.2.2。通过语句“range192.168.2.35 192.168.2.38”可以得到 DHCP 客户能获得的 IP 地址范围是 192.168.2.35～192.168.2.38。

第 9 章 组网技术

9.1 备考指南

9.1.1 考纲要求

根据考试大纲中相应的考核要求，在“组网技术”知识模块上，要求考生掌握以下方面的内容。

(1) 交换机和路由器的基本概念：交换机和路由器的分类、端口，路由表。

(2) 交换机配置：交换机配置方式、交换机的工作模式，基本配置，VLAN 配置，VTP 域的工作模式及配置。

(3) 路由器配置：路由器配置方式、工作模式，接口配置，静态路由和默认路由配置，动态路由协议配置，读懂路由表。

(4) 访问控制列表：IP 访问控制列表的分类、作用及配置。

(5) IPSec 配置：IPSec 实现的工作流程、IPSec 配置。

(6) IPv6 配置：IPv6-over-IPv4 GRE 隧道配置、ISATAP 隧道配置。

(7) 配置广域网接入：配置 PPP 和 DCC、配置帧中继、配置 ISDN。

9.1.2 考点统计

“组网技术”知识模块在历次网络工程师考试试卷中出现的考核知识点及分值分布情况如表 9.1 所示。

表 9.1　历年考点统计表

年　份	题　号	知 识 点	分　值
2017 年下半年	上午：56、66、67、69	交换机及其工作方式	4 分
	下午：试题四	交换机/路由器的配置	15 分
2017 年上半年	上午：56～59、62、63	VLAN 配置、路由器配置	7 分
	下午：试题四	交换机/路由器的配置	15 分
2016 年下半年	上午：19、56～59	路由器配置、网络设备的配置模式、VLAN 配置	5 分
	下午：试题四	交换机/路由器的配置	35 分
2016 年上半年	上午：12、13	交换机的配置、路由器的配置	2 分
	下午：试题二、四	路由器、交换机的配置	35 分
2015 年下半年	上午：23、30、57～59、63	主机路由、静态路由命令，路由器配置，交换机工作原理	6 分
	下午：试题二、四	路由器、交换机配置	35 分
2015 年上半年	上午：10～12、20、24、56、57	交换机配置、路由器、ACL 配置命令	7 分
	下午：试题二、四	交换机配置	15 分
2014 年下半年	上午：11、12、46、48、57、58	思科路由器、交换机配置模式、扩展 ACL 的配置命令、访问控制列表	6 分
	下午：试题三、四	NAT 配置，交换机、路由器配置	15 分
2014 年上半年	上午：11、12、28、29	路由器端口、ip route 命令	4 分
	下午：试题四	在路由器上配置 IPSec VPN	15 分
2013 年下半年	上午：41、23～25	ACL 语句、VTP 协议	8 分
	下午：试题四	交换机的配置、路由器的配置	15 分
2013 年上半年	上午：11、22、28、30	路由器的主要功能，网桥和交换机、路由器的配置	8 分
	下午：试题四	VLAN 配置	20 分
2012 年下半年	上午：28～31	路由器的配置	6 分
	下午：试题四	核心交换机的配置	20 分
2012 年上半年	上午：11、61	三层交换机、ACL 语句	4 分
	下午：试题五	路由器的配置	15 分

9.1.3　命题特点

纵观历年试卷，本章知识点是以选择题和综合分析题的形式出现在试卷中的。本章知识点在历次考试上午试卷中，所考查的题量为 3～5 道选择题，所占分值为 3～5 分（约占试卷总分值 75 分中的 4%～7%)；在下午试卷中，所考查的题量大约为 1 道综合分析题，所占分值大约为 15 分(约占试卷总分值 75 分中的 20%)。大多数试题偏重于实践应用，检验考生是否理解相关的理论知识点和实践经验，考试难度中等偏难。从知识点考查深度的角度分析，每次考试这部分试题在“识记、理解、应用”3 个层面上所占的比例大致为 1∶1∶3。



9.2 考点串讲

9.2.1 交换机基础

9.2.1.1 交换机的作用

局域网交换机工作在数据链路层和网络层，是一种基于 MAC 地址识别来实现数据帧转发功能的一种网络连接设备。它根据进入端口数据帧中的 MAC 地址，过滤、转发数据帧。

交换机拥有许多端口，每个端口都有自己的专用带宽，并且可以连接不同的网段。交换机各个端口之间的通信是同时的、并行的，这就大大提高了信息吞吐量。为了进一步提高性能，每个端口还可以只连接一个设备。为了实现交换机之间的互连或与高档服务器的连接，局域网交换机一般拥有一个或几个高速端口，如 100 Mb/s 以太网端口、FDDI 端口或 155 Mb/s ATM 端口，从而保证整个网络的传输性能。

通过集线器共享局域网的用户不仅是共享带宽，而且是竞争带宽。可能由于个别用户需要更多的带宽而导致其他用户的可用带宽相对减少，甚至被迫等待，因而也就耽误了通信和信息处理。利用交换机的网络微分段技术，可以将一个大型的共享式局域网的用户分成许多独立的网段，减少竞争带宽的用户数量，增加每个用户的可用带宽，从而缓解共享网络的拥挤状况。由于交换机可以将信息迅速而直接地送到目的地，能大大提高速度和带宽，能保护用户以前在介质方面的投资，并能提供良好的可扩展性，因此它不但是网桥的理想替代物，而且是集线器的理想替代物。

局域网交换机的主要功能如下。

- 建立与维护交换表。局域网交换机的交换表表示 MAC 地址与交换机端口所对应的关系。当局域网交换机接收到数据帧时，通过数据帧中的目的 MAC 地址，查询交换表，找到对应的目的交换机端口。
- 建立虚连接。局域网交换机根据已知的源交换机端口(发送节点所在的交换机端口)和通过查询得到的目的交换机端口(目的节点所在的交换机端口)，在两个交换机端口之间建立起虚连接。
- 数据转发。局域网交换机在已经建立好的专用虚通道上完成数据的转发，同时也实现帧过滤、帧传输控制与虚拟网等功能。

9.2.1.2 交换机的分类

交换机有多种分类方法，具体如下。

(1) 按交换方式划分：分为存储转发式交换、直通式交换和碎片过滤式交换。

(2) 根据交换的协议层划分：分为工作在数据链路层的第二层交换机、工作在网络层的第三层交换机、工作在传输层的第四层交换机和多层交换机。

(3) 根据交换机结构划分：分为固定端口交换机和模块化交换机。

(4) 根据配置方式划分：分为堆叠型交换机和非堆叠型交换机。

(5) 根据管理类型划分：分为网管型交换机、非网管型交换机和智能型交换机。

(6) 根据适用范围划分：分为接入层交换机、汇聚层交换机和核心层交换机。

9.2.1.3 交换机的性能指标

交换机的性能指标如下。

(1) 端口类型：双绞线端口、光纤端口、GBIC 端口、SFP 端口。

(2) 传输模式：半双工、全双工、全双工/半双工自适应。

(3) 包转发率：以单位时间内发送 64 字节数据包的个数作为计算基准。

(4) 背板带宽：总带宽=端口数×端口速率×2(全双工模式)。

(5) MAC 地址数：交换机的 MAC 地址表中可以存储的 MAC 地址数量。

(6) VLAN 表项：最大 VLAN 数量反映了一台交换机所能支持的最大 VLAN 数目。

(7) 机架插槽数：机架式交换机所能安插的最大模块数。

9.2.1.4 交换机的工作方式

交换机的工作方式包括静态交换和动态交换两种。目前，交换机最常采用的交换方式是动态交换方式。动态交换模式主要有：存储转发、碎片丢弃和快速转发 3 种模式。

1. 存储转发

所有常规网桥都使用存储转发方法。它们在将数据帧发往其他端口之前，要把收到的帧完全存储在内部的存储器中，对其检验后再发往其他端口，这样其延时就等于接收一个完整的数据帧的时间及处理时间的总和。如果级联很长时，会导致严重的性能问题，但这种方法可以过滤掉错误的数据帧。

2. 碎片丢弃

碎片丢弃交换模式也被称为自由分段模式或碎片隔离交换模式。交换机接收到数据帧后，先检测该数据帧是不是冲突碎片，如果不是冲突碎片，也不保存整个数据帧，而是在接收了它的目的地址就直接进行转发操作；如果该数据帧是冲突碎片，则直接将其丢弃。

3. 快速转发

快速转发只检验数据帧的目标地址，这使得数据帧几乎马上就可以传出去，从而大大降低延时。其缺点是：错误帧也会被传出去。在错误帧的概率较小的情况下，可以采用切入法以提高传输速度；而在错误帧的概率较大的情况下，则可以采用存储转发法以减少错误帧的重传。

9.2.1.5 交换机的工作原理

交换机(二层交换)的工作原理和网桥一样，是工作在链路层的联网设备，它的各个端口都具有桥接功能，每个端口可以连接一个 LAN 或一台高性能网站或服务器，能够通过自学习来了解每个端口的设备的连接情况。所有端口由专用处理器进行控制，并经过控制管理总线转发信息。

例如：节点 A 向节点 B 发送信息，局域网交换机收到 A 节点发出的数据帧后，根据帧中的目的 MAC 地址，查询交换表得到目的端口号，即节点 B 所在的端口号。如果 A 节点

与 B 节点处于交换机的同一个端口上，交换机得到源端口号与目的端口号相同，则出于某种安全控制，将该数据帧丢弃；如果 A、B 节点处于不同的端口且 B 地址在交换表中，则在源端口和目的端口之间建立起虚连接，形成专用的传输通道将该数据帧转发到目的端口；若节点 B 的 MAC 地址不在交换表中，则交换机向 A 节点所处端口以外的所有端口发送一个广播帧，当节点 B 接收到广播帧后会立即做出应答，从而交换机得到节点 B 与其相关联的交换机端口的信息，并将所得到的信息添加到交换表中。然后，再建立虚连接进行数据帧的交换操作。

9.2.1.6　交换表

交换表是交换机进行数据帧交换的基础。交换表的内容包括：目的 MAC 地址、该地址所对应的交换机端口号以及所在的虚拟子网。交换机在初始开机的时候，交换表是空的，使用时，慢慢“学习”建立起它的交换表。

交换表保存在交换机一个有限的高速缓存中，这个高速缓存在一些高端的交换机中。由于高速缓存的空间是有限的，因此交换机必须定时刷新交换表，删去长时间不使用的表项，加入新的表项。

9.2.2　交换机的配置

下面以华为公司的 S5700 系列交换机为例，介绍交换机的一般配置过程。

1. 电缆连接及终端配置

如图 9.1 所示，接好 PC 机和交换机各自的电源线，在关机状态下，把 PC 机的串口 1(COM1)通过控制台电缆与交换机的 Console 端口相连，即完成设备的连接工作。

交换机 Console 端口的默认参数如下。

端口速率：9600b/s。

数据位：8。

奇偶校验码：无。

停止位：1。

流控：无。

在配置 PC 机的超级终端时只需保证端口属性的配置参数与上述参数相同匹配即可。以 Windows 环境下的 Hyper Terminal 为例配置 COM1 端口属性的对话框，如图 9.2 所示。

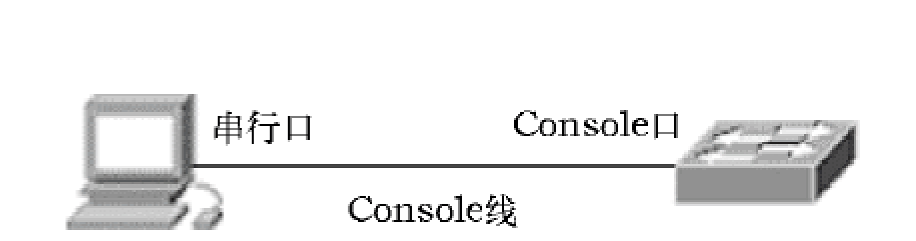


图 9.1　仿真终端与交换机的连接



图 9.2　“COM1 属性”对话框

2. 交换机的启动

在配置好终端仿真软件后，终端窗口就会显示交换机的启动信息，显示交换机的版权信息和软件加载过程，直到出现提示用户设置登录密码。

```
BIOS loading …
…
Enter Password:
Confirm Password:
<HUAWEI>
```

完成 Console 登录密码设置后，用户便可以配置和使用交换机。

3. 交换机的基本配置

在默认配置下，所有接口处于可用状态，并且都属于 VLAN1，这种情况下交换机就可以正常工作了。但为了方便管理和使用，首先应对交换机做基本的配置。

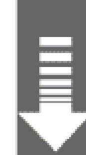
(1) 配置交换机的设备名称、管理 VLAN 和 TELNET，在对网络中交换机进行管理时需要对交换机进行基本配置。

```
<HUAWEI>
<HUAWEI> system-view
[HUAWEI] vlan 5  //创建交换机管理 VLAN 5
[HUAWEI-VLAN5] management-vlan
[HUAWEI-VLAN5] quit
[HUAWEI] interface vlanif 5
[HUAWEI-vlanif5] ip address 10.10.1.1 24
[HUAWEI-vlanif5] quit
[HUAWEI] telnet server enable   //Telnet 出厂时是关闭的，需要打开
[HUAWEI] user-interface vty 0 4   //Telnet 常用于设备管理员登录，推荐使用 AAA 认证
[HUAWEI-ui-vty0-4] protocol inbound telnet    //V2R6 及之前版本缺省支持 telnet 协议，但是 V2R7 及之后版本缺省的是 SSH 协议，因此使用 telnet 登录之前，必须先配置这条命令。
[HUAWEI-ui-vty0-4] authentication-mode aaa
[HUAWEI-ui-vty0-4] idle-timeout 15
[HUAWEI-ui-vty0-4] quit
[HUAWEI] aaa
[HUAWEI-aaa] local-user admin password irreversible-cipher Helloworld@6789
//配置管理员 Telnet 登录交换机的用户名和密码。用户名不区分大小写，密码区分大小写
[HUAWEI-aaa] local-user admin privilege level 15    //将管理员的账号权限设置为15(最高)
[HUAWEI-aaa]local-user admin service-type telnet
[HUAWEI-aaa]quit
[HUAWEI]quit
<HUAWEI>save
```

(2) 登录 Telent 到交换机，出现用户视图提示符。

```
C:\Documents and Settings\Administrator> telnet 10.10.1.1
//输入交换机管理 IP，并回车
Login authentication
Username:admin//输入用户名和密码
```





```
Password:
Info: The max number of VTY users is 5, and the number
of current VTY users on line is 1.
The current login time is 2014-05-06 18:33:18+00:00.
<HUAWEI>
```

(3) 配置交换机的接口。交换机的接口属性默认支持一般网络环境，一般情况下是不需要对其接口进行设置的。在某些情况下需要对其端口属性进行配置时，配置的对象主要有接口隔离、速率、双工等信息。

```
#配置接口 GE1/0/1 和 GE1/0/2 的端口隔离功能，实现两个接口之间的二层数据隔离，三层数据互通
<Switch1>system-view
[Switch1]port-isolate mode 12
[Switch1]interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1]port-isolate enable group 1
[Switch-GigabitEthernet1/0/1]quit
[Switch1]interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2]port-isolate enable group 1
[Switch-GigabitEthernet1/0/2]quit

#配置以太网接口 GE0/0/1 在自协商模式下协商速率为 100Mb/s
<Switch1>system-view
[Switch1] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1]negotiation auto
[Switch-GigabitEthernet1/0/1]auto speed 100

#配置以太网接口 GE0/0/1 在自协商模式下双工模式为全双工模式
<Switch1>system-view
[Switch1] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1]negotiation auto
```

(4) 查看和配置 MAC 地址表。交换机通过学习网络中设备的 MAC 地址，并将学习得到的 MAC 地址存放在交换机的缓存中。在需要向目标地址发送数据时就从 MAC 表地址中查找相应的地址，找到后才可以向目标快速发送数据。

MAC 表由多条 MAC 地址表项组成。MAC 地址表项由 MAC、VLAN 和端口组成，交换机在收到数据帧时，会解析出数据帧的源 MAC 地址和 VLAN ID 并与接收数据帧的端口组合成一条数据表项。MAC 地址表项的查看可以了解交换机运行的状态信息，排查故障。

```
#执行命令 display mac-address，查看所有的 MAC 地址表项
<Switch1>display mac-address
-------------------------------------------------------------------------
MAC Address       VLAN/VSI            Learned-From            Type
-------------------------------------------------------------------------
00e0-0900-7890    10/-                -                     black
00e0-0230-1234    20/-                GE1/0/1                 static
0001-0002-0003    30/-                Eth-Trunk1              dynamic
-------------------------------------------------------------------------
Total items displayed = 3

#执行命令 display interface vlanif5，显示 VLANIF 接口的 MAC 地址
```

```
<Switch1>display interface vlanif5
Vlanif5 current state:DOWN
Line protocol current state:DOWN
Description:
Route Port,Address is 192.168.1.1/24
IP   Sending   Frames'Format   is   PKTFMT_ETHNT_2,Hardware   address   is
00e0-0987-7891
Current system time:2016-07-03 13:33:09+08:00
        Input bandwidth utilization :--
        Output bandwidth utilization :--

#在 MAC 地址表中增加静态 MAC 地址表项，目的 MAC 地址为 0001-0002-0003，VLAN 5 的报文，
从接口 gigabitethernet0/0/5 转发出去
[Switch1]mac-address static 0001-0002-0003 gigabitethernet 0/0/5 vlan 5
```

9.2.3 路由器基础

路由器是工作在 OSI 标准模型的第三层——网络层的数据包转发设备，它通过转发数据包来实现网络互连。路由器通常连接两个或多个由 IP 子网或点到点协议标识的逻辑端口，至少拥有一个物理端口。路由器根据收到的数据包中网络层地址以及路由器内部维护的路由表来决定输出的端口以及下一跳地址，并且通过重写链路层数据包头实现转发数据包。路由器通过动态维护路由表来反映当前的网络拓扑，并通过与网络上其他路由器交换路由和链路信息来维护路由表。

9.2.3.1 路由器的分类

从功能、性能和应用方面划分，路由器分为：骨干路由器、企业级路由器、接入级路由器。

- 骨干路由器是实现主干网络互连的关键设备。
- 企业级路由器连接许多终端，提供通信分类、优先级控制、用户认证等功能。
- 接入级路由器主要用于连接小型企业的客户群。

9.2.3.2 路由器的端口

路由器与广域网连接的端口称为 WAN 端口，路由器与局域网连接的端口称为 LAN 端口。常见的网络端口有以下几种。

(1) RJ-45 端口：通过双绞线连接以太网。

(2) AUI 端口：用在令牌环网或总线型以太网中。

(3) 高速同步串口：用于连接 DDN、帧中继、X.25 和 PSTN 等网络。

(4) ISDN BRI 端口：通过 ISDN 线路实现路由器与 Internet 或其他网络的远程连接。

(5) 异步串口：主要应用于与 Modem 或 Modem 池的连接。

(6) Console 端口：通过配置专用电缆连接至计算机串行口。

(7) AUX 端口：在远程配置时使用。

9.2.3.3 路由器的工作原理

为了实现不同逻辑子网之间的通信，路由器必须具备路由选择和分组转发两个最基本



的功能。

路由选择就是路由器依据目的 IP 地址的网络地址部分，通过路由选择算法确定一条从源节点到达目的节点的最佳路径。路由器的路由选择功能的核心是路由表，它指出了路由器转发数据的最佳路径，决定着数据包是否能够正确地转发到目的主机。

分组转发(Forwarding)通常也称为分组交换(Switching)，它主要完成按照路由选择所指出的路由将数据分组从源节点转发到目的节点。路由器的分组转发过程为：主机将分组发送给默认路由，默认路由器收到分组之后，根据分组中的目的地址查询路由表；路由表中指出该数据分组的传输路径，路由器知道该分组的下一跳路由器的 IP 地址，然后通过地址解析协议 ARP 表，得到与下一跳路由器 IP 地址对应的 MAC 地址，并用该 MAC 地址替换数据分组中的目的 MAC 地址；之后路由器通过数据链路层将数据分组转发给下一跳路由器。

9.2.3.4　路由表

路由表中记录着所有的路由信息，路由器依据路由表给出的信息来确定数据分组的转发路径。路由表的内容主要包括目的网络地址及其所对应的目的端口或下一跳路由器地址和默认路由的信息。如：

```
S 169.105.125.128 [1/0] via 202.112.9.1
```

在路由表中一般第一列为路由源码，它说明该路由表项是通过什么方式、采用什么路由选择协议获得的，如“C”表示直连，“S”表示静态路由，“O”表示使用 OSPF 获得路由信息。

路由表的第二列是目的网络地址和掩码。

路由表的第三列是目的端口或下一跳路由器地址。

路由表中的默认路由表项说明是一条静态路由，它由人工配置，目的网络为 0.0.0.0。0.0.0.0 所表示的是信息没有记录在该路由表中的所有目的地址。

9.2.4　路由器的配置

9.2.4.1　路由器的命令状态

与交换机的配置类似，路由器的配置操作有 3 种模式，即用户视图、系统视图和具体业务视图。用户视图模式下，在用户视图下，用户可以完成查看运行状态和统计信息等功能，这些命令对路由器的正常工作没有影响；在系统视图模式下，用户可以配置系统参数以及通过该视图进入其他的功能配置视图；在具体业务视图模式下，用户可以配置接口相关的物理属性、链接层特性及 IP 地址等重要参数，路由协议的大部分参数也需要在这种模式下配置。其中，配置模式又分为全局配置模式和接口配置模式、路由协议配置模式、线路配置模式等子模式。在不同的工作模式下，路由器有不同的命令提示状态。

- <Switch>。在交换机正常启动后，用户使用终端仿真软件或 Telent 登录交换机，可自动进入用户配置模式，这时用户可以看路由器的连接状态，访问其他网络和主机，但不能看到和更改路由器的设置内容。
- [Switch]。路由器处于系统视图命令状态，在<Switch>提示符下输入 system-view，

可进入系统视图状态，这时不仅可以执行所有的用户命令，还可以看到和更改路由器的设置内容。

- [Switch-vlan]。路由器处于具体的业务视图状态，在[Swith]提示符下输入需要配置的业务命令，可进入该状态。退出具体的业务输入 quit。

在开机自检时，按 Ctrl+Break 组合键可进入 BootROM menu 状态，这时路由器不能完成正常的功能，只能进行软件升级和手工引导，或者进行路由器口令恢复时要进入该状态。

9.2.4.2 路由器的基本配置

配置 enable 口令、enable 密码和主机名，在路由器中同样可以配置启用口令(enable password)和启用密码(enable secret)，一般情况下只需配置一个就可以，当两者同时配置时，后者生效。这两者的区别是，启用口令以明文显示，而启用密码以密文形式显示。主机名及路由器口令的设置和上一节对交换机配置的主机名及口令相同，这里不再赘述。

配置路由器以太网接口，路由器一般提供一个或多个以太网接口槽，每个槽上会有一个以上以太网接口。以太网接口因此而命名为{Ethernet 槽位/端口}或{GigabitEthernet 槽位/端口}，例如 Ethernet0/0、GigabitEthernet0/0/1，也可缩写为 Eth0/0、GE0/0/1。

对以太网接口做如下配置：

```
#设置系统的日期、时间和时区
<Huawei>clock timezone BJ add 08:00:00
<Huawei>clock datetime 20:10:00 2015-03-26

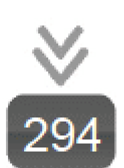
#设置设备名称和管理 IP 地址
<Huawei>system-view
[Huawei]sysname Server
[Server]interface gigabitethernet 0/0/0
[Server-GigabitEthernet0/0/0]ip address 10.137.217.177 24
[Server-GigabitEthernet0/0/0]quit

#设置 Telnet 用户的级别和认证方式
[Server] telent server enable
[Server] user-interface vty 0 4
[Server-ui-vty0-4]user privilege level 15
[Server-ui-vty0-4]authentication-mode aaa
[Server-ui-vty0-4]quit
[Server]aaa
[Server-aaa]  local-user  admin1234  password  irreversible-cipher
Helloworld@6789
[Server-aaa] local-user admin1234 privilege level 15
[Server-aaa] local-user admin1234 service-type telent
[Server-aaa]quit
```

由于同一厂商的网络设备往往采用一种网络操作平台，交换机、路由器的配置以及命令的使用都是相似的。

9.2.5 配置广域网接入

如果要将网络与其他远程网络连接起来，有时要用到广域网(NVAN)接入服务。本节结





合具体的 PPP、帧中继 FR 和 ISDN BRI 连接接入实例来学习广域网接入的配置方法和技巧。

9.2.5.1　配置 PPP 和 DCC

点对点协议是作为在点对点链路上进行 IP 通信的封装协议而被开发出来的。PPP 定义了 IP 地址的分配和管理、异步和面向位的同步封装、网络协议复用、链路配置、链路质量测试和错误检测等标准，以及网络层地址协议和数据压缩协议等协议标准。PPP 通过可扩展的链路协议和网络控制协议(NCP)来实现上述功能。

PPP 具有多协议支持的特点，可以支持 IP、IPX 和 DECnet 等第三层协议。PPP 提供了安全认证机制，这主要是通过 PAP(口令认证协议)和 CHAP(挑战握手协议)来实现的。PAP 和 CHAP 被用来认证是否允许对端设备进行拨号连接。

多链路 PPP 是 PPP 的另一项功能，它允许在路由器和路由器之间或路由器和拨号的 PC 之间建立多条链路，通信量在这些链路之间进行负载均衡，从而提高了可用带宽和链路的可靠性。

按需拨号路由(Dial Control Center，DCC)是利用拨号链路实现网络间互连的一种常用技术。其主要功能是将数据包从被拨号的接口进行路由；决定何种数据包可以触发拨号；触发拨号：决定什么时候终止连接。DCC 技术和 PPP 技术一样对于 ISDN 的配置是非常重要的，在实际应用中 ISDN、PPP 和 DCC 这三项技术经常综合使用。

相关命令及说明如表 9.2 所示。

表 9.2　PPP 的相关配置命令

命　令	功　能
interface mp-group	创建 MP-Group 接口并进入 MP-Group 接口视图
local-user user-name password	创建本地账号，并配置本地账号的登录密码
local-user user-name service-type ppp	配置本地用户使用的服务类型为 PPP
ppp authentication-mode{chap|pap}[[call-in]domain domain-name	配置本端设备对端设备的认证方式
authentication-scheme scheme-name	建立认证方案
domain domain-name	配置默认域
ppp chap user username	配置采用 CHAP 认证时认证方的用户名
ppp mp mp-group number	物理接口加入指定的组

9.2.5.2　配置帧中继

帧中继是一种高性能的 WAN 协议，运行在 OSI 参考模型的物理层和数据链路层。它是一种数据包交换技术，是 X.25 的简化版本。它省略了 X.25 的一些强健功能，如提供窗口技术和数据重发技术，而是依靠高层协议提供纠错功能，这是因为帧中继工作在更好的 WAN 设备上，这些设备较之 X.25 的 WAN 设备具有更可靠的连接服务和更高的可靠性，它严格地对应于 OSI 参考模型的最低两层，而 X.25 还提供第三层的服务，所以帧中继比 X.25 具有更高的性能和更有效的传输效率。

帧中继广域网的设备分为 DTE 和 DCE。DTE 表示数据终端设备，DCE 表示数据通信设备，用于将用户 DTE 设备接入网络。

帧中继技术提供面向连接的数据链路层通信，在每对设备之间都存在一条定义好的通信链路，且该链路有一个链路识别码。这种服务通过帧中继虚电路实现，每个帧中继虚电路都以数据链路识别码(DLCI)标识自己。DLCI 的值一般由帧中继服务提供商指定。帧中继既支持 PVC 也支持 SVC。

其相关命令及说明如表 9.3 所示。

表 9.3　帧中继的相关配置命令

命　令	功　能
link-protocol fr	设置 Frame Relay 封装
fr interface-type dte	设置 Frame Relay 接口类型 DTE
fr dlci dlci	配置帧中继链路的数据连接标识符
fr map ip	配置本端 DLCI 到对端 IP 地址的静态映射

9.2.5.3　配置 ISDN

综合业务数字网(Integrated Service Digital Network，ISDN)是电话网络数字化的结果，由数字电话和数据传输服务两部分组成，可以在 ISDN 上传输声音、数据和视频等多种信息。ISDN 组件包括终端、终端适配器、网络终端设备、线路终端设备和交换终端设备等。

ISDN 提供了两种类型的访问接口，即基本速率接口(Basic Rate Interface，BRI)和主要速率接口(Primary Rate Interface，PRI)。ISDN BRI 提供两个 B 信道和一个 D 信道(2B+D)。ISDN 的 B 信道为承载信道，其速率为 64Kb/s，用于传输用户数据；D 信道速率为 16Kb/s，主要用于传输控制信息。PRI 提供 30 个 B 信道和一个 D 信道(30B+D)，其 B 信道和 D 信道的速率均为 64Kb/s。

其相关命令及说明如表 9.4 所示。

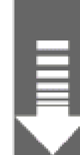
表 9.4　ISDN 的相关配置命令

命　令	功　能
dialer-rule	进入 Dialer-rule 视图
dialer-rule dialer-rule-number {acl{acl-number|name acl-name}|ip{deny|permit}|ipv6{deny|permit}}	配置某个拨号访问组对应的拨号访问控制列表，指定引发 DCC 呼叫的条件
dialer enable-cricular	使能轮询 DCC 功能
interface bri interface-number	进入指定的 ISDN BRI 接口
display isdn call-info [interface interface-type interface- number]	查看 ISDN 接口的当前呼叫状态
isdn ststistics{clear|continue|display[flow]|start|stop}	ISDN 接口信息统计

9.2.6　IPv6 配置与测试

9.2.6.1　IPv6-over-IPv4 GRE 隧道配置

IPv6-over-IPv4 隧道是将 IPv6 报文封装在 IPv4 报文中，让 IPv6 数据包穿过 IPv4 网络进行通信。对于采用隧道技术的设备来说，在隧道的入口处，将 IPv6 的数据报封装进 IPv4，



IPv4 报文的源地址和目的地址分别是隧道入口和隧道出口的 IPv4 地址：在隧道的出口处，再将 IPv6 报文取出转发到目的节点。隧道技术只要求在隧道的入口和出口处进行修改，对其他部分没有要求，容易实现。但是，隧道技术不能实现 IPv4 主机与 IPv6 主机的直接通信。

使用标准的 GRE 隧道技术，可以在 IPv4 的 GRE 隧道上承载 IPv6 数据报文。GRE 隧道是两点之间的连路，每条连路都是一条单独的隧道。GRE 隧道把 IPv6 作为乘客协议，将 GRE 作为承载协议。所配置的 IPv6 地址是在 Tunnel 接口上配置的，所配置的 IPv4 地址是 Tunnel 的源地址和目的地址(隧道的起点和终点)。

IPv6-over-IPv4GRE 隧道的相关配置命令及功能如表 9.5 所示。

表 9.5　GRE 隧道的相关配置命令及功能

命　令	功　能
interface tunnel interface-numbe	创建 Tunnel 接口
tunnel-protocol gre	指定 Tunnel 为 GRE 模式
source {ip-addresslinterface-type interface-number}	指定 Tunnel 的源地址或源接口
ipv6 enable	使能接口的 IPv6 功能
ipv6 address {ipv6-addressprefix-lengthlipv6-address/prefix-leng20	设置 Tunnel 接口的 IPv6 地址

9.2.6.2　SATAP 隧道配置

站内自动隧道寻址协议(Intra-Site Automatic Tunnel Addressing Protocol，ISATAP)过渡技术采用了双栈和隧道技术实现从 IPv4 向 IPv6 的过渡。ISATAP 隧道是点到点的自动隧道技术，它将 IPv4 地址置入 IPv6 地址中，当两台 ISATAP 主机通信时，可自动抽取出 IPv4 地址建立 Tunnel 通信，并且不需要通过其他特殊网络设备，只要彼此间 IPv4 网络通畅即可。

当双栈主机使用 ISATAP 隧道时，IPv6 报文的目的地址和隧道接口的 IPv6 地址都要采用特殊的地址-ISATAP 地址。ISATAP 地址格式为 Prefix (64bit)：0:5EFE:IPv4ADDR，其中，0:5EFE 是 IANA 规定的格式，IPv4ADDR 是单播 IPv4 地址，它嵌入到 IPv6 地址的低 32 位。ISATAP 地址的前 64 位是通过向 ISATAP 路由器发送请求得到的，如果需要和其他网络的 ISATAP 客户端或者 IPv6 网络通信，必须通过 ISATAP 路由器拿到全球单播地址前缀(2001:、002:、3ffe:开头)，通过路由器与其他 IPv6 主机和网络通信。

ISATAP 隧道可以用于 IPv4 网络中 IPv6 路由器与 IPv6 路由器、主机与路由器的连接。由于不要求隧道节点具有全球唯一的 IPv4 地址，可以用于内部私有网络中各双栈主机进行 IPv6 通信，所以 ISATAP 隧道适用于 IPv4 网络中 IPv6 主机之间的通信或 IPv4 网络中 IPv6 主机接入到 IPv6 网络的通信。ISATAP 隧道的相关配置命令及功能如表 9.6 所示。

表 9.6　ISATAP 隧道相关配置命令及功能

命　令	功　能
tunnel-protocol ipv6-ipv4 isatap	配置 Tunnel 接口的隧道协议为 ipv6-ipv4 并使用 isatap 隧道
ipv6 address 2001::/64 eui-64	配置接口的 EUI-64 格式的全球单播地址
source gigabitethemet 2/0/0	用来配置 Tunnel 源地址或源接口
undo ipv6 nd ra halt1	用来使能系统发布 RA 报文功能
netsh interface ipv6 isatap set router	用来为用户端添加静态路由(windows)
display ipv6 interface Tunnel 0/0/2	用来查看接口的 IPv6 信息

9.2.7 访问控制列表

9.2.7.1 ACL 的基本概念

IP 访问控制列表的过滤功能，提供了基于源地址、目的地址、各种协议和端口号的过滤准则。设定不同的过滤准则，不但能够实现拒绝接收或允许接收某些源 IP 地址的数据包进入路由器，也可以拒绝接收或允许接收到达某些目的 IP 地址的数据包通过路由器，还可以拒绝接收或允许接收某些协议的数据包通过路由器，拒绝接收或允许接收某些协议的某些端口号的数据包通过路由器。

IP 访问控制列表主要有两种类型：一类是标准访问控制列表(IP Standard Access List)，另一类是扩展访问控制列表(IP Extended Access Lists)。

标准访问控制列表只对数据包中的源地址进行检查，而不考虑目的地址及端口号等过滤选项，表号为 1～99。

扩展访问控制列表除了检查源地址和目的地址外，还可以检查指定的协议，根据数据包头中的协议类型进行过滤；还可以检查端口号，根据端口号对数据包进行过滤。扩展访问控制列表的表号范围是 100～199，后来又进行了扩展，扩展的表号是 2000～2699。

配置访问控制列表的最关键命令是 permit 和 deny。它们用来表示满足访问表项的报文是允许通过接口，还是要过滤掉。permit 表示允许报文通过接口，而 deny 表示匹配标准 IP 访问表源地址的报文要被丢弃掉。访问控制列表的条件语句是从第一句开始顺序执行的，只有与这个判断不相符合，才继续往下执行条件语句。例如我们要过滤 IP 地址为 202.112.23.9 的数据包，来自其他 IP 地址的数据包都被允许通过路由器，我们应该先执行判断这个数据包的 IP 地址是否是 202.112.23.9，即“deny 202.112.23.9”，再允许其他 IP 地址的数据包通过，即“permit any any”。如果将 permit 语句放在 deny 语句的前面，那么在执行第一句语句时，即使是来自 IP 地址为 202.112.23.9 的数据包，也将通过这个路由器，并且不再往下执行语句，我们将不能过滤来自主机地址 198.78.46.8 的报文。

访问控制列表的配置工作主要包括：先定义一个标准、扩展或命名的访问控制列表；接着为该访问控制列表配置包过滤的准则；最后为这个访问控制列表配置应用接口。

9.2.7.2 ACL 配置命令

使用编号(2000～2999)创建一个数字型的基本 ACL，并进入基本 ACL 视图，操作命令如下。

```
acl [ number ] acl-number [ match-order { auto | config } ]
```

或者使用名称创建一个命名型的基本 ACL，并进入基本 ACL 视图操作命令为：

```
acl name acl-name { basic| acl-number } [ match-order { auto | config } ]
```

如果创建 ACL 时未指定 match-order 参数，则该 ACL 默认的规则匹配顺序为 config；创建 ACL 后，ACL 的默认步长为 5。如果该值不能满足管理员部署 ACL 规则的需求，则可以对 ACL 步长值进行调整；(可选)执行命令 description text，配置 ACL 的描述信息。

配置基本 ACL 的规则的操作命令如下。





```
rule [ rule-id ] { deny | permit } [ source { source-address source-wildcard
| any } |vpn-instance
vpn-instance-name | [ fragment | none-first-fragment ] | logging | time-range
time-name ]
```

以上步骤仅是一条 permit/deny 规则的配置步骤。实际配置 ACL 规则时，需根据具体的业务需求，决定配置多少条规则以及规则的先后匹配顺序。

1) ACL 语句的删除

删除 ACL，系统视图下执行命令：

```
undo acl { [ number ] acl-number | all } 或 undo acl name acl-name
```

一般可以直接删除 ACL，不受引用 ACL 的业务模块影响(简化流策略中引用 ACL 指定 rule 的情况除外)，即无须先删除引用 ACL 的业务配置。

2) 调整 ACL 步长

在网络维护过程中，需要管理员为原 ACL 添加新的规则。由于 ACL 的默认步长是 5，在系统分配的相邻编号的规则之间，最多只能插入 4 条规则。调整步长，在 ACL 视图下执行 step，配置 ACL 步长。

3) 查看与清除 ACL 信息

确认设备 ACL 资源的分配情况，在任意视图下查看 ACL 资源信息的命令如下。

```
display acl resource [ slot slot-id ]
```

若显示信息中的计数非零，表示设备仍存在空余的 ACL 资源。

确认需要清除 ACL 的运行信息后，在用户视图下清除 ACL 统计信息的命令如下。

```
reset acl counter { name acl-name | acl-number | all }
```

4) 通配符掩码

ACL 规定使用通配符掩码来说明子网地址，通配符掩码就是子网掩码按位取反的结果。通配符掩码 0.0.0.0 表示 ACL 语句中的 32 位地址要求全部匹配，因而叫作主机掩码。例如：192.168.1.1 0.0.0.0 表示主机 192.168.1.1 的 IP 地址，实际上路由器把这个地址转换为 host 192.168.1.1，注意这里的关键字 host。

通配符掩码 255.255.255.255 表示任意地址都是匹配的，通常与地址 0.0.0.0 一起使用，例如：0.0.0.0 255.255.255.255，路由器将把这个地址转换为关键字 any。表 9.7 给出了几个使用通配符掩码的例子。

表 9.7　通配符掩码的例子

IP 地址	通配符掩码	匹　配
0.0.0.0	255.255.255.255	匹配任何地址(关键字 any)
172.16.1.1	0.0.0.0	匹配 host 172.16.1.1
172.16.1.0	0.0.0.255	匹配子网 172.16.1.0/24
172.16.2.0	0.0.1.255	匹配子网 172.16.2.0/23 (172.16.2.0-172.16.3.255)
172.16.0．0	0.0.255.255	配子网 172.16.0.0/16 (172.16.0.0-172.16.255.255)

9.3 真题详解

9.3.1 综合知识试题

试题 1 (2017 年下半年试题 56)

以下关于直通交换的叙述中，正确的是＿(56)＿。

(56) A. 比存储转发交换速率要慢
B. 存在坏帧传播的风险
C. 接收到帧后简单存储，进行 CRC 校验后快速转发
D. 采用软件方式查找站点转发

参考答案：(56)B。

要点解析：直通交换只检查数据包的包头，获取目的地址，即可传出去，延时小、交换速度快，但其缺点是数据包无须存储，无法检查所传送的数据包是否有误，不具备错误检测能力。因此存在坏帧传播的风险。

试题 2 (2017 年下半年试题 66)

关于华为交换机设置密码，正确的说法是＿(66)＿。

① 华为交换机的缺省用户名是 admin，无密码
② 通过 BootRoom 可以重置 Console 口密码
③ Telnet 登录密码丢失，通过 Console 口登录交换机后重新进行配置
④ 通过 Console 口登录交换机重置 BootRoom 密码

(66)A.①②③④　B. ②③④　C.②③　D.①③④

参考答案：(66)C。

要点解析：华为交换机可以通过 Telnet 登录交换机修改 Console 口密码，也可以通过 BootRoom 清除 Console 口密码后再修改。若 Telnet 密码或 Web 密码丢失可以通过 Console 口登录交换机后重新进行配置；若 BootRoom 密码丢失，可以通过 Console 口登录交换机后重置。华为设备的 Web 登录界面默认用户名是 admin，而从 Console 接口进入的用户没有默认用户名。

试题 3 (2017 年下半年试题 67)

观察交换机状态指示灯是初步判断交换机故障的检测方法，以下关于交换机状态指示灯的描述中，错误的是＿(67)＿。

(67) A. 交换机指示灯显示红色表明设备故障或者告警，需要关注和立即采取行动
B. STCK 指示灯绿色表示接口在提供远程供电
C. SYS 指示灯亮红色表明交换机可能存在风扇或温度告警
D. 交换机业务接口对应单一指示灯，常亮表示连接，快闪表示数据传送

参考答案：(67)B。



要点解析：STCK(STACK，堆叠)指示灯绿色表示业务指示灯暂时用来指示设备堆叠信息，即本设备为堆叠设备或堆叠从设备。

试题 4 （2017 年下半年试题 69）

两台交换机的光口对接，其中一台设备的光 UP，另一台设备的光口 DOWN。定位此类故障的思路包括__(69)__。

① 光纤是否交叉对接

② 两端使用的光模块波长和速率是否一样

③ 两端通信端口是否都设置为光口

④ 两个光口是否未同时配置自协商或者强制协商

(69)A. ①②③④　B. ②③④　C. ②③　D. ①③④

参考答案：(69)A。

要点解析：定位此类故障首先应查看光纤是否成对，存在不存在交叉对接的情况；其次通过命令行查看光模块参数，确定波长和速率是否相同；然后再通过命令行查看接口状态，端口工作模式是否都设置为光口模式；最后查看两个光口是否未同时配置自协商或强制协商。

试题 5 （2017 年上半年试题 56）

查看 VLAN 配置信息的命令是__(56)__。

(56) A. displaycurrent-configuration　　B. displayvlanbrief

C. system-view　　D. vlanvlan-id

参考答案：(56)A。

要点解析：查看配置信息的命令是 displaycurrent-configuration。

试题 6 （2017 年上半年试题 57）

运行 RIPv2 协议的 3 台路由器按照如图 9.3 所示的方式连接，路由表项最少需经过__(57)__可达到收敛状态。

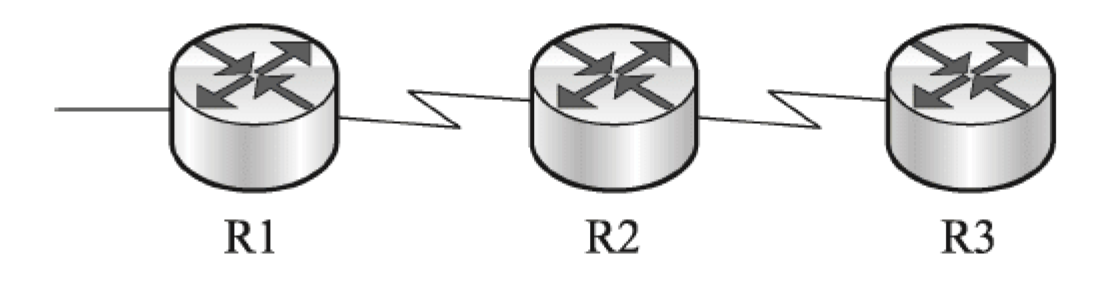


图 9.3　路由器连接

(57)A. 30s　B. 60s　C. 90s　D. 120s

参考答案：(57)B。

要点解析：RIP 协议的特点：①只和相邻路由器交换信息。②交换的信息是本路由器知道的所有信息，也就是路由表。③每隔 30 秒发整张路由表的副表到邻居路由器。在本题中，经过 60s 的时候所有路由器就能学到所有的网段信息。

试题 7 （2017 年上半年试题 58）

运行 OSPF 协议的路由器在选举 DR/BDR 之前，DR 是__(58)__。

(58) A. 路由器自身　　B. 直连路由器

C. IP 地址最大的路由器　　　　　D. MAC 地址最大的路由器

参考答案：(58)A。

要点解析：在运行 OSPF 路由协议的广播多路型网络中，初始阶段 OSPF 路由器会在 HELLO 包里将 DR 和 BDR 指定为 0.0.0.0，当路由器收到邻居路由器的 HELLO 包时，就会检查 HEELO 包里携带的路由器优先级，DR 和 BDR 等字段，然后列举出具备 DR 和 BDR 资格的路由器。

试题 8 (2017 年上半年试题 59)

关于 OSPF 路由协议的说法中，正确的是__(59)__。

(59) A. OSPF 路由协议是一种距离矢量路由协议
B. OSPF 路由协议中的进程号全局有效
C. OSPF 路由协议不同进程之间可以进行路由重分布
D. OSPF 路由协议的主区域为区域

参考答案：(59)C。

要点解析：OSPF 是链路状态路由协议，进程号只具备本地意义，主干区域号为 0，不同的 OSPF 进程是可以进行重发布的。

试题 9 (2017 年上半年试题 62 和试题 63)

在缺省配置时交换机所有端口__(62)__，不同 VLAN 的数据帧必须通过__(63)__传输。

(62) A. 属于直通状态　　　　B. 属于不同 VLAN
C. 属于同一 VLAN　　　　D. 地址都相同

(63) A. DNS 服务器　　　　B. 路由器
C. 二层交换机　　　　D. DHCP 服务器

参考答案：(62)C；(63)B。

要点解析：默认情况下交换机的所有端口属于同一 VLAN，不同 VLAN 间的通信需要通过三层设备。

试题 10 (2016 年下半年试题 19)

连接终端和数字专线的设备 CSU/DSU 被集成在路由器__(19)__端口中。

(19) A. RJ-45 端口　　B. 同步串口　　C. AUI 端口　　D. 异步串口

参考答案：(19)B。

要点解析：通道服务单元/数据服务单元(CSU/DSU)是用于连接终端和数字专线的设备，而且 CSU/DSU 属于 DCE(Data Communication Equipment，数据通信设备)。目前 CSU/DSU 通常都被集成在路由器的同步串口之上，而且 CSU/DSU 被整合在一起，是一个硬件设备。

试题 11 (2016 年下半年试题 56)

下面的提示符__(56)__表示特权模式。

(56) A. >　　B. #　　C. (config)#　　D. !

参考答案：(56)B。

要点解析：用户模式>：在 Cisco 设备启动工作完成之后，即进入用户模式，只允许基本的监测命令，比如 ping 其他网络设备，在这种情况下不能改变路由器的配置。



特权模式#：用户模式下输入 enable 命令，可进入特权模式。在特权模式下，可以使用 show 命令来观察设备的状况和我们所做的配置。在特权模式下不能对设备进行配置。

全局模式(config)#：在特权模式下输入 config terminal 命令即可进入全局模式。在全局模式下可以对网络设备进行配置，并且在全局模式下所做的配置对整个设备都有效。

如果需要对某个接口进行单独的配置，就需要从全局模式进入这个接口子模式。

试题 12　(2016 年下半年试题 57)

把路由器当前配置文件存储到 NVRAM 中的命令是__(57)__。

(57) A. Router(config)#copy currentto starting
　　B. Router#copy starting to running
　　C. Router(config)#copy running-config starting-config
　　D. Router#copy run startup

参考答案：(57)D。

要点解析：把路由器当前配置文件存储到 NVRAM 中的命令可以用 Router#copy run startup。D 选项为缩写，实际上是 copy running-config startup-config，该命令需在特权模式下配置。

试题 13　(2016 年下半年试题 58)

如果路由器显示“Serial 1 is down, line protocol is down”故障信息，则问题出在 OSI 参考模型的__(58)__。

(58) A. 物理层　　B. 数据链路层　　C. 网络层　　D. 会话层

参考答案：(58)A。

要点解析：接口信息显示中 Serial 1 is down, line protocol is down，第一个 down 是物理层状态，第二个 down 是数据链路层状态，该信息说明物理层故障进而导致 line protocol down，并不能判定 line protocol 是否真正 down 了。故答案为 A。

试题 14　(2016 年下半年试题 59)

下面的交换机命令中__(59)__为端口指定 VLAN。

(59) A. S1(config-if)#vlan-membership static
　　B. S1(config-if)#vlan database
　　C. S1(config-if)#switchport mode access
　　D. S1(config-if)#switchport access vlan 1

参考答案：(59)D。

要点解析：在默认配置下，所有的接口都处于可用状态且均属于 VLAN1，采用静态配置法配置 VLAN，也就是说在交换机上手动将某个端口分配给一个 VLAN。所用命令为 S1(config-if)#switchport access vlan 1。

试题 15　(2016 年上半年试题 12)

以下关于以太网交换机地址学习机制的说法中，错误的是__(12)__。

(12) A. 交换机的初始 MAC 地址表为空
　　B. 交换机接收到数据帧后，如果没有相应的表项，则不转发该帧

C. 交换机通过读取输入帧中的源地址添加相应的 MAC 地址表项

D. 交换机的 MAC 地址表项是动态变化的

参考答案：(12)B。

要点解析：交换机接收到数据帧后，如果没有相应的表项，将广播发送帧。

试题 16 (2016 年上半年试题 13)

路由器包含多种端口以连接不同类型的网络设备，其中能够连接 DDN、帧中继、X.25 和 PSTN 等广域网络的是__(13)__。

(13) A. 同步串口　　B. 异步串口

C. AUX 端口　　D. Consol 端口

参考答案：(13)A。

要点解析：常见的路由器的端口有：

① RJ-45 端口：通过双绞线连接以太网。

② AUI 端口：用在令牌环网或总线型以太网中。

③ 高速同步串口：用于连接 DDN、帧中继、X.25 和 PSTN 网络。

④ ISDN BRI 端口：通过 ISDN 线路实现路由器与 Internet 或其他网络的远程连接。

⑤ 异步串口：主要应用于与 Modem 或 Modem 池的连接。

⑥ Console 端口：通过配置专用电缆连接至计算机串行口。

⑦ AUX 端口：在远程配置时使用。

试题 17 (2015 年下半年试题 23)

下面 4 种路由中，哪一种路由的子网掩码是 255.255.255.255？__(23)__

(23) A. 远程网络路由　　B. 主机路由

C. 默认路由　　D. 静态路由

参考答案：(23)B。

要点解析：因特网所有的分组转发都是基于目的主机所在的网络，但在大多数情况下都允许有这样的特例，即对特定的目的主机指明一个路由。这种路由就叫作特定主机路由。

试题 18 (2015 年下半年试题 30)

如果要将目标网络为 202.117.112.0/24 的分组经 102.217.115.1 接口发出，需增加一条静态路由，正确的命令是__(30)__。

(30) A. Route add 202.117.112.0 255.255.255.0 102.217.115.1

B. Route add 202.117.112.0 0.0.0.255 102.217.115.1

C. add route 202.117.112.0 255.255.255.0 102.217.115.1

D. add route 202.117.112.0 0.0.0.255 102.217.115.1

参考答案：(30)A。

要点解析：添加静态路由的格式是：

route add [-net|-host] [网络或主机] netmask [mask] [gw|dev]

试题 19 (2015 年下半年试题 57)

配置路由器接口的提示符是__(57)__。



(57) A. router (config)#　　B. router (config-in)#
C. router (config-intf)#　　D. router (config-if) #

参考答案：(57)D。

要点解析：路由器的基本配置如下。

① 进入特权模式

```
Router>                      (用户模式提示符)
Router> enable               (进入特权模式)
Password:<password>          (输入口令)
Router#                      (特权模式提示符)
```

② 进入全局配置模式

```
Router# ip routing           (启动路由协议)
Router# config terminal      (输入 config termial 命令进入配置模式)
Router(config)#              (配置模式提示符)
```

③ 配置接口

```
Router(config)# interface fastethernet0/1  (进入接口 F0/1 子配置模式)
Router(config-if)# ip address 192.168.0.1 255.255.255.0
(设置该接口的 IP 地址，格式为：ip address ip-addr subnet-mask)
Router(config-if)# no shutdown             (激活接口)
Router(config-if)# exit                    (返回至全局配置模式)
```

如果有多个接口需配置，则重复步骤③。

④ 查看配置，保存配置

```
Router(config)# end                        (退回到特权模式)
Router# Show running-config                (查看配置)
Router# write                              (保存配置)
```

试题 20　(2015 年下半年试题 58)

如果想知道配置了哪种路由协议，应使用的命令是__(58)__。

(58) A. Router>showrouter protocol
B. Router (config)>show ip protocol
C. Router (config)>#show router protocol
D. Router >show ip protocol

参考答案：(58)D。

要点解析：show 命令可以同时在用户模式和特权模式下运行，“show ？”命令用来提供一个可利用的 show 命令列表。show ip protocol 表示查看当前路由器运行的动态路由协议情况。

试题 21　(2015 年下半年试题 59)

如果在互联网中添加了一个局域网，要用手工方式将该局域网添加到路由表中，应使用的命令是__(59)__。

(59) A. Router(config)>ip route 2.0.0.0 255.0.0.0 via 1.0.0.2
B. Router(config)#ip route 2.0.0.0 255.0.0.0 1.0.0.2

C. Router (config) #ip route 2.0.0.0 via 1.0.0.2

D. Router (config) #ip route 2.0.0.0 1.0.0.2 mask 255.0.0.0

参考答案：(59)B。

要点解析：该命令格式为：

Router(config)# ip route network [mask] {address|interface} [distance] [permanent]

[distance] [permanent]是配置浮动静态路由的选项。浮动静态路由是一种特殊的静态路由，通过配置一个比主路由的管理距离更大的静态路由，保证网络中主路由失效的情况下，提供备份路由。但在主路由存在的情况下它不会出现在路由表中。

{address|interface}，在静态的添加到达目的网络的路由的时候，可以指定路径中下一台设备的地址，也可以指定与下一台设备连接的自己这台路由器的接口。

试题 22 (2015 年下半年试题 63)

以下关于交换机获取与其端口连接设备的 MAC 地址的叙述中，正确的是__(63)__。

(63) A. 交换机从路由表中提取设备的 MAC 地址

B. 交换机检查端口流入分组的源地址

C. 交换机之间互相交换地址表

D. 由网络管理员手工输入设备的 MAC 地址

参考答案：(63)B。

要点解析：交换机刚刚连接到以太网时，其转发表是空的。这时若交换机收到一个帧，它将怎样处理呢？交换机就按照自学习(self-learning)算法处理收到的帧(这样就逐步建立起转发表)，并且按照转发表把帧转发出去。这种自学习算法的原理并不复杂，因为：若从某个站 A 发出的帧从接口 x 进入了某交换机，那么从这个接口出发沿相反方向一定可以把一个帧传送到 A。所以交换机只要每收到一个帧，就记下其源地址和进入交换机的接口，作为转发表中的一个项目。

9.3.2 案例分析试题

试题 1 (2017 年下半年下午试题四)

【说明】

某公司网络拓扑图如图 9.4 所示。

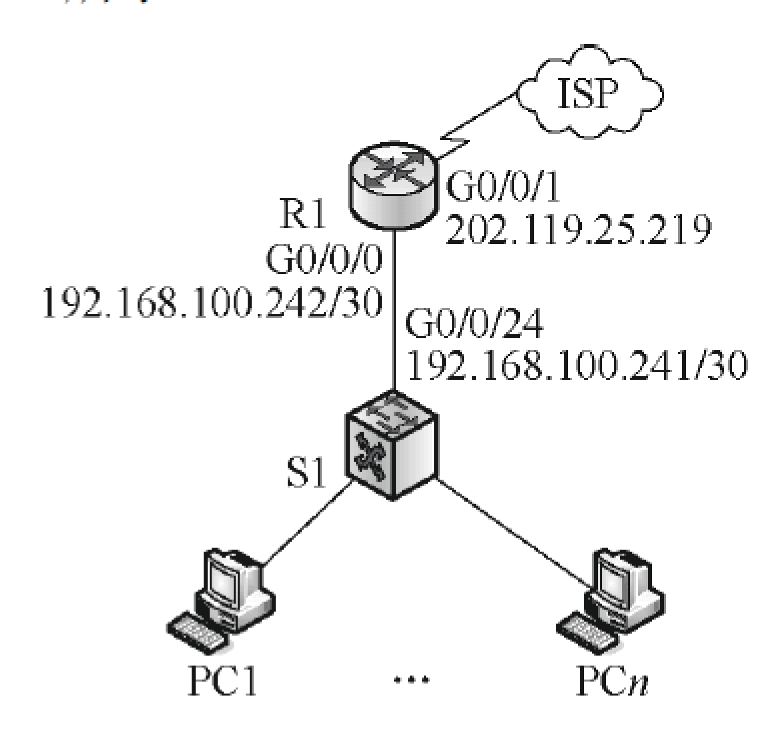


图 9.4 某公司网络拓扑图



【问题 1】(5 分)

为了便于管理公司网络，管理员根据不同部门对公司网络划分了 VLAN，VLAN 编号及 IP 地址规划如表 9.8 所示。考虑到公司以后的发展，每个部门的 IP 地址规划均留出了一定的余量。请根据需求，将表 9.8 补充完整。

表 9.8 VLAN 编号及 IP 地址规划

部 门	VLAN 编号	主机数量	IP 地址范围	子网掩码
行政部门	VLAN100	32	192.168.100.129～__(1)__	__(2)__
营销部门	VLAN105	68	192.168.100.1～192.168.100.126	255.255.255.128
财务部门	VLAN110	8	192.168.100.193～192.168.100.222	__(3)__
后勤部门	VLAN115	8	__(4)__～192.168.100.238	255.255.255.240

公司计划使用 24 接口的二层交换机作为接入层交换机，根据以上主机数量在不考虑地理位置的情况下，最少需要购置__(5)__台接入层交换机。

【问题 2】(10 分)

公司申请了 14 个公网 IP 地址，地址范围为 202.119.25.209～202.119.25.222。其中，202.119.25.218～202.119.25.222 作为服务器和接口地址保留，其他公网 IP 地址用于公司访问 Internet。公司使用 PAT 为营销部门提供互联网访问服务。请根据描述，将下面配置代码补充完整。

```
<Huawei>system-view
[Huawei]__(6)__R1
[R1]user-interface__(7)__ //进入 console 用户界面视图
[R1-ui-console0]authentication-mode__(8)__
Please configure the login password (maximum length 16): huawei
[R1-ui-console0]quit
[R1]int GigabitEthernet, 0/0/0
[R1-GigabitEthernet0/0/0]ipaddres s192.168.100.242 255.255.255.252
[R1-GigabitEthernet0/0/0]__(9)__
[R1]__(10)__2000
[R1-acl-2000]__(11)__5 permit source 192.168.100.0__(12)__
[R1-acl-basic-2000]quit
[R1]nat address-group 1__(13)__202.119.25.217
[R1]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet 0/0/1]ip address__(14)__255.255.255.240
[R1-GigabitEthernet 0/0/1]__(15)__outbound 2000 address-group1
[R1]rip
[R1-rip-1]version 2
[R1-rip-1]network 192.168.100.0
交换机配置略…
```

参考答案：

【问题 1】

(1)192.168.100.190；(2)255.255.255.192；(3)255.255.255.240；(4)192.168.100.225；(5)5。

【问题 2】

(6)sysname；(7)console 0；(8)password；(9)quit；(10)acl；(11)rule (12)0.0.0.255；(13)202.119.25.209；(14)202.119.25.219；(15)NAT。

要点解析：

【问题 1】由图形说明可知，行政部需要 32 个有效主机地址，因此分配主机位位数为 6，网络号位数则为 26，对应子网掩码为 255.255.255.192，对应的网段为 192.168.100.128，最后一个有效 IP 地址为 192.168.100.1011 1110，即 192.168.100.190。同理可求得其他部门的 IP 及子网掩码。

主机数量一共有 32+68+8+8=116(台)，不考虑位置，则需要接入交换机(24 接口)116/24=4.8，至少需要 5 台交换机。

【问题 2】

[Huawei] sysname R1 表示配置设备名为 R1。

[R1]user-interface console 0 表示进入 Console 用户界面视图，参数 interface-number 用来指定 Console 口编号，只能为 0。

登录 Console 用户界面的验证方式。当用户通过 Console 口登录交换机时终端会提示输入登录密码，登录交换机。使用 quit 命令可以退出当前模式，空(10)[R1] acl 2000 语句定义了一个标准 ACL 2000。

[R1-acl-2000] rule 5 permit source 192.168.100.0 0.0.0.255，该语句表明允许源地址为 192.168.100.1～192.168.100.254 的数据包通过，其中 192.168.100.0/24 是该网络的网络地址，子网掩码是 255.255.255.0，而 ACL 的子网掩码用反向子网掩码即 0.0.0.255。

空(13)所在语句意义为配置 IP 地址池 1，包括两个公网地址 202.119.25.209 和 202.119.25.217。

```
[R1]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet 0/0/1]ip address 202.119.25.219 255.255.255.240
[R1-GigabitEthernet 0/0/1] nat outbound 2000 address-group1
```

此处语句的意义为在出接口 GigabitEthernet 0/0/1 上配置 ACL 2000 与 IP 地址池 1 相关联。

试题 2 (2017 年上半年下午试题四)

【说明】

图 9.5 为某学校网络拓扑图，运营商分配的公网 IP 地址为 113.201.60.1/29，运营商网关地址为 113.201.60.1，内部用户通过路由器代理上网，代理地址为 113.201.60.2。核心交换机配置基于全局的 DHCP 服务，在办公楼和宿舍楼用户提供 DHCP 服务。内部网络划分为 3 个 VLAN，其中 VLAN10 的地址为 10.0.10.1/24，VLAN20 的地址为 10.0.20.1/24，VLAN30 的地址为 10.0.30.1/24，请结合图 9.5，回答相关问题。

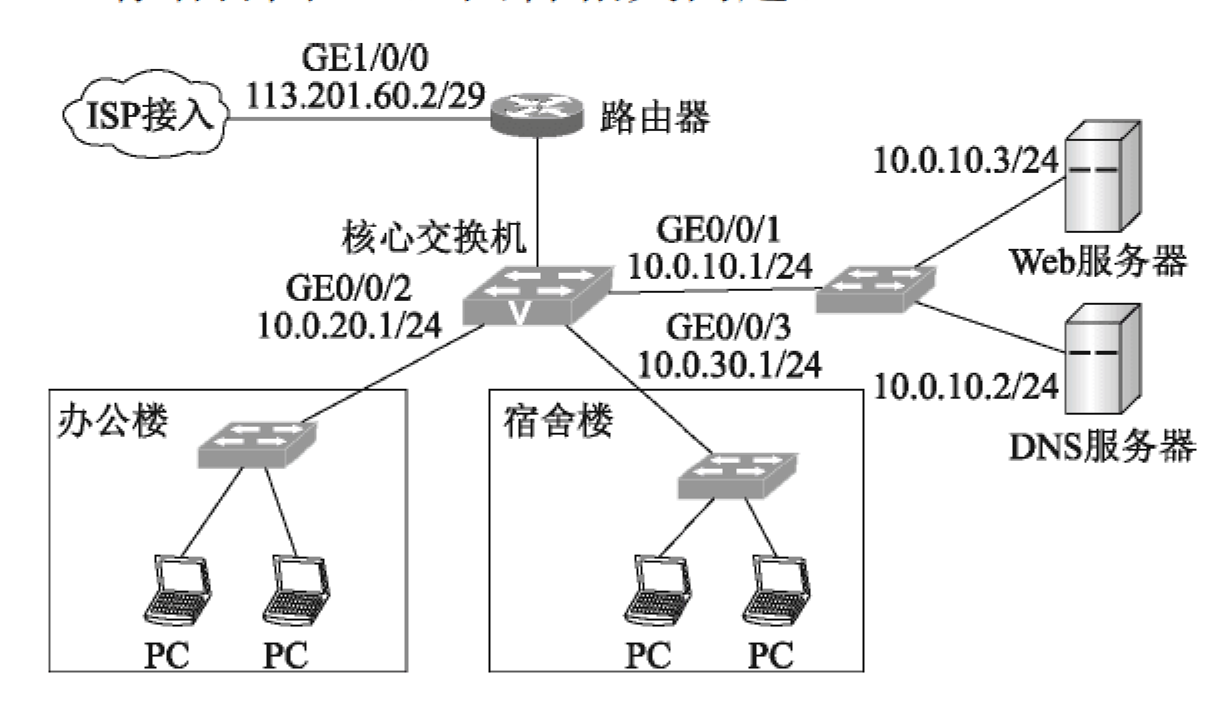


图 9.5　某学校网络拓扑图

【问题 1】(共 9 分)

路由器的配置片段如下，根据图 9.5，补齐(1)～(6)空缺的命令。

```
#配置 WAN 接口和内网上网代理
&lt;Huawei&gt;system-view
[Huawei]sysname__(1)__
[Router]interface__(2)__
[Router-Gigabit Ethernet1/0/0]ip address__(3)__
[Router-Gigabit Ethernet1/0/0]quit
[Router]ip route-static 0.0.0.0 0.0.0__(4)__
[Router-acl-basic-2000]
[Router-acl-basic-2000]rule 5 permit source10.0.0.0__(5)__
[Router-acl-basic-2000]quit
[Router]interface Gigabit Ethernet1/0/0
[Router-Gigabit Ethernet1/0/0]nat outbound__(6)__
[Router-Gigabit Ethernet1/0/0]quit
…
其他配置略
```

【问题 2】(共 6 分)

核心交换机的配置片段如下，根据图 9.5，补齐(7)～(10)空缺的命令。

```
#配置 GEO/0/2 接口加入 VLAN20，并配置对应 VLAN 接口地址
[Switch]vlan batch 20
[Switch]interface Gigabit Ethernet0/0/2
[Switch-GigabitEthernet0/0/2]port link-type__(7)__
[Switch-GigabitEthernet0/0/2]port hybrid pvid vlan 20
[Switch-GigabitEthernet0/0/2]port hybrid untagged vlan 20
[Switch-GigabitEthernet0/0/2]quit
[Switch]interface vlanif20
[Switch-Vlanif20]ipaddress__(8)__
[Switch-Vlanif20]quit
…
```

其他配置略。

```
#配置 DHCP 服务，租期 3 天
[Switch]dhcp__(9)__
[Switch]ip pool pooll
[Switch-ip-pool-pooll]network 10.0.20.0 mask 225.225.255.0
[Switch-ip-pool-pooll]dns-list 10.0.10.2
[Switch-ip-pool-pooll]gateway-list 10.0.20.1
[Switch-ip-pool-pooll]lesae day__(10)__
[Switch-ip-pool-pooll]quit
[Switch]interface vlanif 20
[Switch-Vlanif20]dhcp select global
[Switch-Vlanif20]quit
…
```

其他配置略。

参考答案:

【问题1】

(1)Router；(2)GigabitEthernet 1/0/0；(3)113.201.60.2；255.255.255.248；(4)113.201.60.1；(5)0.0.255.255；(6)2000。

【问题2】

(7)hybrid；(8)10.10.20.1 255.255.255.0；(9)enable；(10)3。

要点解析:

【问题1】

(1)重命名设备。

(2)进入端口子模式。

(3)给端口配置 IP 和掩码。

(4)配置默认路由，下一跳指向 ISP 地址。

(5)配置反掩码。

(6)把符合 ACL2000 的地址做 NAT 转换。

【问题2】

(7)除了 Access 类型和 Trunk 类型外，交换机还支持第三种 Hybird 类型端口。这种接口可以接收和发送多个 VLAN 数据帧，同时还能指定对任何 VLAN 帧进行剥离标签操作。

(8)配置接口 IP 和掩码。

(9)dhcp enable：开启 dhcp 配置。

(10)lease day 3：配置租约期为 3 天。

试题3 (2016年下半年下午试题四)

【说明】

某公司建立局域网拓扑图如图 9.6 所示。公司计划使用路由器作为 DHCP 服务器，根据需求，公司内部使用 C 类地址段，服务器地址段为 192.168.2.0/24，S2 和 S3 分别为公司两个部门的接入交换机。分别配置 VLAN 10 和 VLAN 20，地址段分别使用 192.168.10.0/24 和 192.168.20.0/24，通过 DHCP 服务器自动为两个部门分配 IP 地址，地址租约期为 12 小时。其中，192.168.10.1～192.168.10.10 作为保留地址。

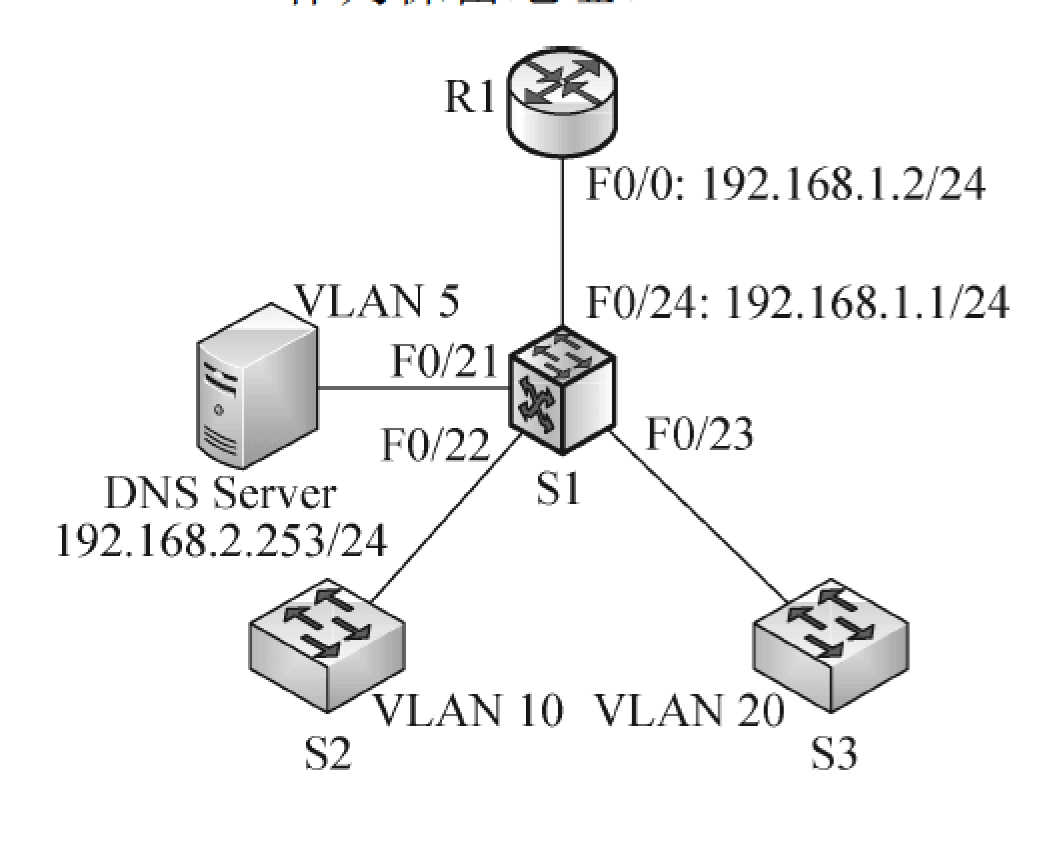


图 9.6　局域网拓扑网



【问题 1】(10 分，每空 1 分)

下面是 R1 的配置代码，请将下面配置代码补充完整。

```
R1#config t
R1(config)#interface FastEthernet0/0
R1(config-if)#ip address (1)  (2)
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#ip dhcp (3) depart1
R1(dhcp-config)#network 192.168.10.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.10.254 255.255.255.0
R1(dhcp-config)#dns-server (4)
R1(dhcp-config)#lease 0  (5)  0
R1(dhcp-config)#exit
R1(config)#ip dhcp pool depart2
R1(dhcp-config)#network (6)  (7)
R1(dhcp-config)#default-router 192.168.20.254 255.255.255.0
R1(dhcp-config)#dns-server 192.168.2.253
R1(dhcp-config)#lease 0 12 0
R1(dhcp-config)#exit
R1(config)#ip dhcp excluded-address
R1(config)#ip dhcp excluded-address (8)  (9)
R1(config)#ip dhcp excluded-address (10) //排除掉不能分配的 IP 地址
R1(config)#ip dhcp excluded-address 192.168.20.254
```

【问题 2】(5 分，每空 1 分)

下面是 S1 的配置代码，请将下面配置代码或解释补充完整。

```
S1#config terminal
S1(config)#interface vlan 5
S1(config-if)#ip address 192.168.2.254 255.255.255.0
S1(config)#interface vlan 10
S1(config-if)#ip helper-address (11)   //指定 DHCP 服务器的地址
S1(config-if)#exit
S1(config)#interface vlan 20
…
S1(config)#interface f0/24
S1(config-if)#switchport mode (12)
S1(config-if)#switchport trunk (13) vlan all  //允许所有 VLAN 数据通过
S1(config-if)#exit
S1(config)#interface f0/21
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 5
S1(config-if)#exit
S1(config)#interface f0/22
S1(config-if)#switchport mode access
S1(config-if)#switchport access (14)
S1(config)#interface f0/23
S1(config-if)#switchport mode access
S1(config-if)#switchport access (15)
```

参考答案：

【问题 1】

(1)192.168.1.2；(2)255.255.255.0；(3)pool；(4)192.168.2.253；



(5)12；(6)192.168.20.0；(7)255.255.255.0；(8)192.168.10.1；
(9)192.168.10.10；(10)192.168.10.254。

【问题2】

(11)192.168.1.2；(12)trunk；(13)allowed；(14)vlan10；(15)vlan20。

要点解析：

【问题1】

根据网络拓扑图可知F0/0的IP地址为192.168.1.2，子网掩码为255.255.255.0。空(3)表示设置DHCP地址池，空(4)为设置DNS服务器地址，即192.168.2.253，空(5)R1(dhcp-config)#lease 0 12 0表示设定DHCP地址租约为12小时，空(6)、(7)表示部门2使用192.168.20.0/24，设置VLAN20的网络地址R1(dhcp-config)#network 192.168.20.0 255.255.255.0，其中192.168.10.1～192.168.10.10地址保留不分配，所以：

```
R1(config)#ipdhcp excluded-address 192.168.10.1  192.168.10.10
R1(config)#ipdhcp excluded-address 192.168.10.254 //排除掉不能分配的IP地址
```

【问题2】

S1(config-if)#ip helper-address 192.168.1.2　//指定DHCP服务器的地址

该企业使用路由器作为DHCP服务器，故所填地址即为路由器的地址。trunk模式的端口用于交换机与交换机，交换机与路由器，大多用于级联网络设备。access多用于接入层也叫接入模式，主要是将端口静态接入。默认情况下trunk允许所有的VLAN通过，即S1(config-if)# switchport trunk allowed vlan all　//允许所有VLAN数据通过。由题意知，部门1使用的是VLAN 10，interface f0/22，部门2使用的是VLAN 20，interface f0/23，所以空(14)填写vlan 10，空(15)填写vlan 20。

试题4 (2016年上半年下午试题二)

【说明】

某学校的网络拓扑结构图如图9.7所示。

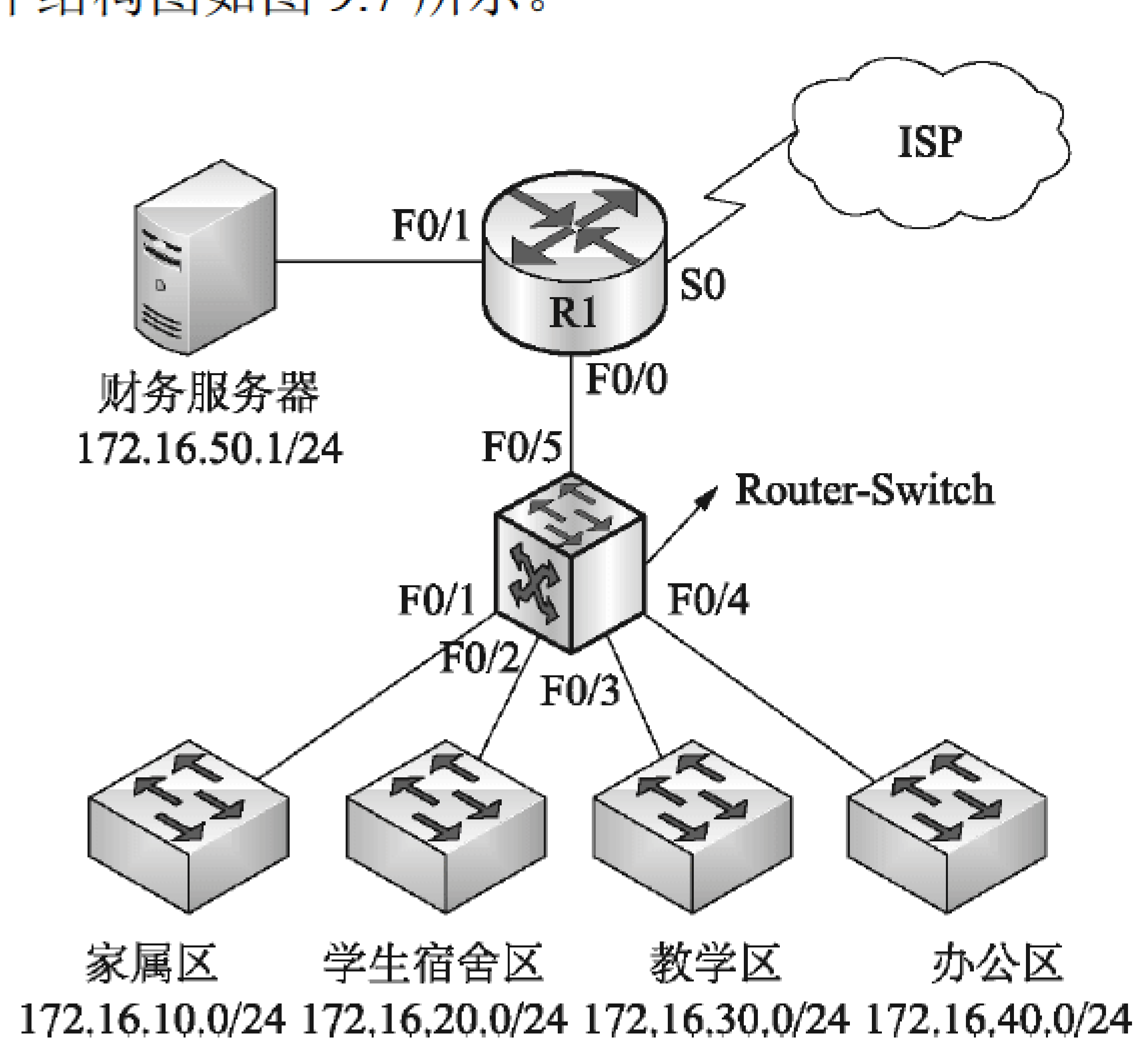


图9.7　某学校网络拓扑结构图



【问题 1】(每空 1 分，共 7 分)

常用的 IP 访问控制列表有两种，它们是编号为__(1)__和 1300～1399 的标准访问控制列表和编号为__(2)__和 2000～2699 的扩展访问控制列表。其中，标准访问控制列表是根据 IP 报文的__(3)__来对 IP 报文进行过滤，扩展访问控制列表是根据 IP 报文的__(4)__、__(5)__、上层协议和时间等来对 IP 报文进行过滤。一般来说，标准访问控制列表放置在靠近__(6)__的位置，扩展访问控制列表放置在靠近__(7)__的位置。

【问题 2】(每空 1 分，共 10 分)

为保障安全，使用 ACL 对网络中的访问进行控制。访问控制的要求如下。

(1) 家属区不能访问财务服务器，但可以访问互联网。

(2) 学生宿舍区不能访问财务服务器，且在每天 18:00～24:00 禁止访问互联网。

(3) 办公区可以访问财务服务器和互联网。

(4) 教学区禁止访问财务服务器，且每天 8:00～18:00 禁止访问互联网。

1. 使用 ACL 对财务服务器进行访问控制，请将下面配置补充完整。

```
R1(config)#access-list1__(8)__ __(9)__0. 0. 0. 255
R1(config)#access-list1 deny 172.16.10.0 0.0.0.255
R1(config)#access-list1 deny 172.16.20.0 0.0.0.255
R1(config)#access-list1 deny __(10)__0.0.0.255
R1(config)#interface__(11)__
R1(config-if)#ip access-group1__(12)__
```

2. 使用 ACL 对 Internt 进行访问控制，请将下面配置补充完整。

```
Route-Switch(config)#time-rangejxq//定义教学区时间范围
Route-Switch(config-tune-range)#periodic daily__(13)__
Route-Switch(config)#time-range xsssq//定义学生宿舍区时间范围
Route-Switch(config-time-range)#periodic__(14)__18:00 to 24:00
Route-Switch(config-time-range)#exit
Route-Switch(config)#access-list 100 permit ip 172.16.10.0 0.0.0.255 any
Route-Switch(config)#access-list 100 permit ip 172.16.40.0 0.0.0.255 any
Route-Switch(config)#access-list 100 deny ip__(15)__0.0.0.255 time-rangejxq
Route-Switch(corffig)#access-list 100 deny ip__(16)__0.0.0.255 time-rangexsssq
Route-Switch(config)#interface__(17)__
Route-Switch(config-if)#ip access-group 100 out
```

【问题 3】(每空 1 分，共 3 分)

网络在运行过程中发现，家属区网络经常受到学生宿舍区网络的 DDoS 攻击，现对家属区网络和学生宿舍区网络之间的流量进行过滤，要求家属区网络可访问学生宿舍区网络，但学生宿舍区网络禁止访问家属区网络。

采用自反访问列表实现访问控制，请解释配置代码。

```
Route-Switch(config)#ip access-list extended infilter
Route-Switch(config-ext-nacl)#permit ip any 172.16.20.0 0.0.0.255 refiectjsq__(18)__
Route-Switch(config-ext-nacl)#exit
Route-Switch(config)#ip access-list extended outfilter
Route-Switch(config-ext-nacl)#evaluate jsq__(19)__
Route-Switch(config-ext-nacl)#exit
Route-Switch(config)#interface faste thernet 0/1
```

```
Route-Switch(config-if)#ip access-group infilter in
Route-Switch(config-if)#ip access-group outfilter out//_(20)_
```

参考答案：

【问题1】

(1)1～99；(2)100～199；(3)源地址；(4)源地址；(5)目的地址；(6)数据目的地；(7)数据源。

【问题2】

(8)permit；(9)172.16.40.0；(10)172.16.30.0；(11)F0/1；(12)out；(13)8:00 to 18:00；(14)daily；(15)172.16.30.0；(16)172.16.20.0；(17)F0/5。

【问题3】

(18)当符合任何网络访问 172. 16. 20. 0/16 网络的数据流通过的时候，建立自反控制列表 jsp。

(19)计算并生成自反列表。

(20)在接口 F0/1 出口方向上应用这个自反列表。

要点解析：

【问题1】

目前常用的 ACL 有两种，分别是标准 ACL 和扩展 ACL，其中，标准 ACL 使用 1～99 以及 1300～1999 之间的数字作为表号，扩展 ACL 使用 100～199 以及 2000～2699 之间的数字作为表号。这两种 ACL 的区别是，标准 ACL 只检查数据包的源地址；扩展 ACL 既检查数据包的源地址，也检查数据包的目的地址，同时还可以检查数据包的特定协议类型、端口号等。因此，在实际使用中，标准 ACL 的配置位置要尽量靠近目的端，扩展 ACL 的配置位置要尽量靠近源端，这样才能起到最好的效果。

【问题2】

题目要求可以归纳为禁止 IP 地址为 172.16.10.0/24(家属区)、172.16.20.0/24(学生宿舍区)、172.16.30.0/24(教学区)访问 172.16.50.1/24(财务服务器)；允许 IP 地址为 172.16.40.0/24(办公区)访问 172.16.50.1/24；172.16.10.0/24 和 172.16.40.0/24 可以一直访问互联网；172.16.20.0/2 每天 18:00 到 24:00 禁止访问互联网；172.16.30.0/24 每天 8:00 到 18:00 禁止访问互联网。

```
禁止某网络地址访问的命令为:access-list[ACL 表号]deny[ip][mask];
允许某网络地址访问的命令为:access-list[ACL 表号]permit[ip][mask];
R1 (config)#access-list1(permit)(172.616.40.0)0. 0. 0. 255,permit 语句,允许来自办公区的数据访问;
教学区禁止访问财务服务器用 deny 语句拒绝教学区的 IP 地址;
R1 (config)#interface F0/1 //进去 R1 的 F0/1 端口,不能是 F0/0 接口,以免家属区等不能访问互联网;
R1 (config-if)#ipaccess-group1out//将 ACL1 设置到 F0/1 端口上,在财务服务器的端口,设置上这个 ACL 表,就可以完成对财务服务器的访问控制了。
```

要通过 ACL 来限制用户在规定的时间范围内访问特定的服务，首先设备上必须配置好正确的时间范围。时间范围是通过配置 time-range 来实现的。

```
oute-Switch(config)#access-list 100 deny ip 172.16.30.00.0.0.255 time-range jxq //教学区按 jxq 时间范围禁止访问互联网,教学区 IP 地址为 172.16.30.0;
```



```
Route-Switch(config)#access-list  100  deny  ip  172.16.40.00.0.0.255
time-range xsssq //学生宿舍区按 xsssq 时间范围禁止访问互联网，教学区 IP 地址为
172.16.40.0;
Route-Switch(config)#interface 0/5 //F0/5 端口是交换机连接路由器的端口
Route-Switch(config-if)#ipaccess-group 100 out //将 ACL100 设置到 F0/5 端口上。
```

【问题 3】

根据题意要求在 172.16.10.0/24 的网段上添加对于 172.16.20.0/24 网段的自反访问列表。

自反访问列表 Reflexive Access Lists，根据一个方向的访问控制列表，自动创建出一个反方向的控制列表，是和原来的控制列表的 IP 的源地址和目的地址颠倒，并且源端口号和目的端口号完全相反的一个列表。并且还有一定的时间限制，过了时间，就会超时，一旦超时，这个新创建的列表就会消失，这个方法能大大增加安全性。

```
Route-Switch(config)#ip access-list extended infilter //建立名为 infilter 的
访问策略，因为这个策略准备设置在流量的入口，取名为 infilter;
Route-Switch(config-ext-nacl)#permit ip any 172.16.20.0 0.0.0.255 reflect
jsq //当符合任何网络访问 172.16.20.0/16 网络的数据流通过的时候，建立自反控制列表 jsp;
Route-Switch(config-ext-nacl)#evaluate jsq//计算并生成自反列表;
Route-Switch(config-if)#ip access-group outfilter out//在接口 F0/1 出口方向上
应用这个自反列表。
```

试题 5 （2016 年上半年下午试题四）

【说明】

某公司有 3 个分支机构，网络拓扑结构及地址分配如图 9.8 所示。

【问题 1】(每空 1 分，共 11 分)

公司申请到 202. 111. 1. 0/29 的公有地址段，采用 NAPT 技术实现公司内部访问互联网的要求，其中，192. 168. 16. 0/22 网段禁止访问互联网。R1、R2 和 R3 的基本配置已正确配置完成，其中 R1 的配置如下。请根据拓扑结构，完成下列配置代码。

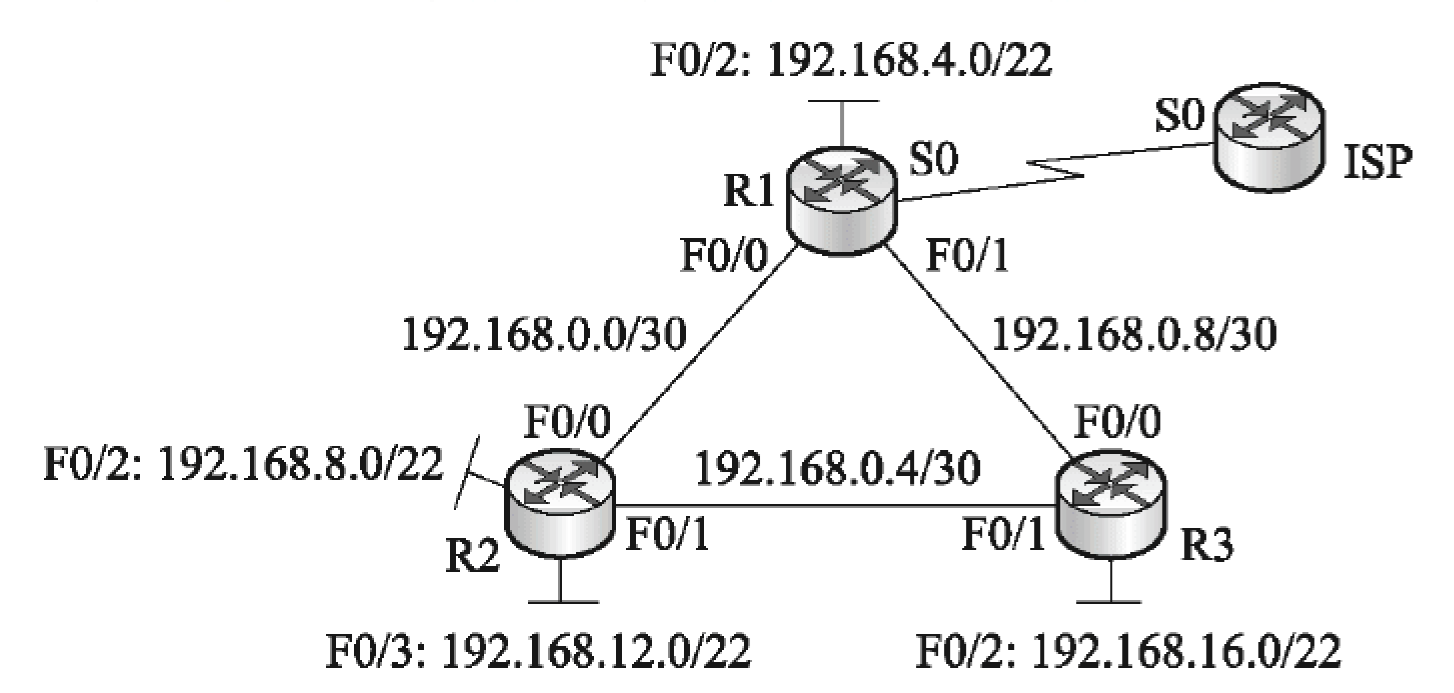


图 9.8　某公司网络拓扑结构

R1 的基本配置及 NAPT 配置如下：

```
R1>enable
R1#configtenminal
R1(config)#interface fastenthernet 0/0
R1(config-if)#ip address192.168.0.1 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#exit
```

```
R1(config)#interface fastenthernet 0/1
R1(config-if)#ip address 192.168.0.9  255.255.255.252
R1(config-if)#noshutdown
R1(config-if)#exit
R1(config)#interface fastenthernet 0/2
R1(config-if)#ip address__(1)__255.255.252.0//使用网段中最后一个地址
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface serial0
R1(config-if)#ip address 202.111.1.1 255.255.255.248
R1(config-if)#noshutdown
R1(config)#ip nat pool ss 202.111.1.1__(2)__netmask__(3)__
R1(config)#interface__(4)__fastenthernet 0/0-1
R1(config-if)#ipnat__(5)__
R1(config-if)#interface serial0
R1(config-if)#ipnat__(6)__
R1(config-if)#exit
R1(config)#access-listl permit 192.168.0.0__(7)__
R1(config)#ipnatinside__(8)__list__(9)__pool__(10)__ __(11)__
```

【问题 2】(每空 2 分，共 4 分)

在 R1、R2 和 R3 之间运行 OSPF 路由协议，其中 R1、R2 和 R3 的配置如下。

行号	配置代码
1	R1(config)#router ospf1
2	R1(config-router)#network 192.168.4.0 0.0.3.255 area 0
3	R1(config-router)#network 192.168.0.0 0.0.0.3 area 0
4	R1(config-router)#network 192.168.0.8 0.0.0.3 area 0
5	R2>enable
6	R2#config terminal
7	R2(config)#router ospf2
8	R2(config-router)#network 192.168.8.0 0.0.3.255 area 0
9	R2(config-router)#network 192.168.12.0 0.0.3.255 area 0
10	R2(config-router)#network 192.168.0.4 0.0.0.3 area 0
11	R3>enable
12	R3#configterminal
13	R3(config)#router ospf 3
14	R3(config-router)#network 192.168.0.8 0.0.0.3 area 0
15	R3(config-router)#network 192.168.0.4 0.0.0.3 area 0

1. 配置完成后，在 R1 和 R2 上均无法 ping 通 R3 的局域网，可能的原因是__(12)__。

(12)备选答案：

A. 在 R3 上未宣告局域网路由

B. 以上配置中第 7 行和第 13 行配置错误

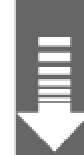
C. 第 1 行配置错误

D. R1、R2 未宣告直连路由

2. 在 OSPF 中重分布默认路由的命令是：__(13)__。

(13)备选答案：

A. R1#default-information originate



B. R1(config-if)#default-information originate

C. R1(config-router)#default-information originate

D. Rl(config)#default-information originate

参考答案：

【问题 1】

(1)192.168.7.254；(2)202.111.1.6；(3)255.255.255.248；(4)range；(5)inside；(6)outside；(7)0.0.15.255；(8)source；(9)1；(10)ss；(11)overload。

【问题 2】

(12)A；

(13)C。

要点解析：

【问题 1】

题目给出了网段 192.168.4.0/22，据此计算出此网址的最后一个能用的 IP 地址是 192.168.7.254。

R1(config)#ip nat pool ss 202.111.1.1(202.111.1.6)netmask(255.255.255.248)

地址池名字为 ss，起始 IP 地址为 201.111.1.1，终止 IP 地址是 202.111.1.6，255. 255. 255. 248 是地址池的子网掩码。

inter f0/1 是进入一个接口；interface range f0/1 也是进入一个接口；如果 range 后面只有一个接口，这时候这两个命令作用一样，没有区别，但实际上通常情况下 range 的作用是一次进入多个接口。

ip nat inside 是指定与内部网络相连的内部端口，ip nat outside 是指定与外部网络相连的外部端口。

R1(config)#access-list1permit192.168.0.0(0.0.15.255)，这是访问控制列表 ACL 的语句 access-list1 表示这是 ACL 1，permit 表示允许 192.168.0.0 段主机通过这个规则，其他的都拒绝，子网掩码是 255.255.240.0，通配符局是 0.0.15.255。

R1(config)#ip nat inside(source)list(1)pool(ss)(overload)//定义了一个地址池名称为 ss，还定义了一个标准访问控制列表，编号为 1，然后将该访问控制列表与地址池进行关联。ip nat inside source list * pool *，这是将访问控制列表与地址池进行关联的固定格式。overload 表明复用外网接口地址。

【问题 2】

根据题目给出的相关配置可知，R1 和 R2 均无法 ping 通 R3 的局域网，表明在 R1 和 R2 上不存在 R3 局域网的路由条目，最可能的原因是在 R3 上未宣告其局域网路由。

在 OSPF 路由协议中，重分布默认路由的命令是在路由协议配置模式先使用 default-information originate 命令。

试题 6 （2015 年下半年下午试题二）

【说明】

某企业的网络结构如图 9.9 所示。

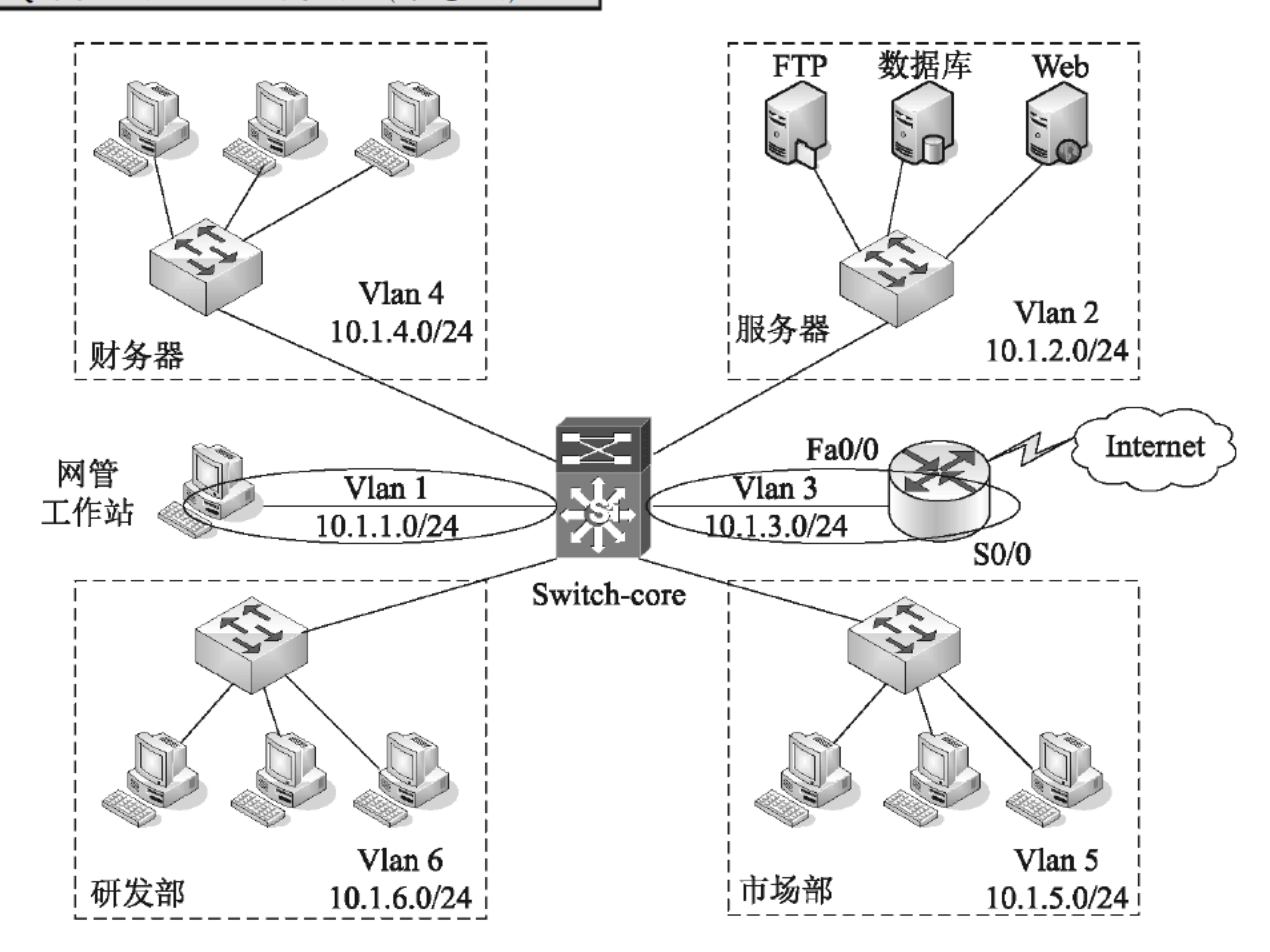


图 9.9　某企业网络拓扑图

该企业通过一台路由器接入到互联网，企业内部按照功能的不同分为 6 个 VLAN。分别是网络设备与网管(VLAN1)、内部服务器(VLAN2)、Internet 连接(VLAN3)、财务部(VLAN4)、市场部(VLAN5)、研发部门(VLAN6)。

【问题 1】(7 分)

1. 访问控制列表 ACL 是控制网络访问的基本手段，它可以限制网络流量，提高网络性能。ACL 使用<u>(1)</u>技术来达到访问控制目的。 ACL 分为标准 ACL 和扩展 ACL 两种，标准访问控制列表的编号为<u>(2)</u>和 1300～1999 之间的数字，标准访问控制列表只使用<u>(3)</u>进行过滤，扩展的 ACL 的编号使用<u>(4)</u>以及 2000～2699 之间的数字。

2. 每一个正确的访问列表都至少应该有一条<u>(5)</u>语句，具有严格限制条件的语句应放在访问列表所有语句的最上面，在靠近<u>(6)</u>的网络接口上设置扩展 ACL，在靠近<u>(7)</u>的网络接口上设置标准 ACL。

【问题 2】(5 分)

网管要求除了主机 10.1.6.66 能够进行远程 Telnet 到核心设备外，其他用户都不允许进行 Telnet 操作。同时只对员工开放 Web 服务器(10.1.2.20)、FTP 服务器(10.1.2.22)和数据库服务器(10.1.2.21:1521)，研发部除 IP 为 10.1.6.33 的计算机外，都不能访问数据库服务器，按照要求补充完成以下配置命令。

```
Switch-core# conf t
Switch-core(config)#access-list 1 permit host  (8)
Switch-core(config)#line  (9)  0 4
Switch-core(config-line)#access-class 1  (10)
…
Switch-core(config)#ip access-list extend server-protect
```



```
Switch-core(config-ext-nacl)#permit tcp host ___(11)___ host 10.1.2.21 eq 1521
Switch-core(config-ext-nacl)#deny tcp ___(12)___ 0.0.0.255 host 10.1.2.21 eq 1521
Switch-core(config-ext-nacl)#permit tcp 10.1.0.0 0.0.255.255 host 10.1.2.21 eq 1521
Switch-core(config-ext-nacl)#permit tcp 10.1.0.0 0.0.255.255 host 10.1.2.20 eq www
Switch-core(config-ext-nacl)#permit tcp 10.1.0.0 0.0.255.255 host 10.1.2.22 eq ftp
…
```

【问题 3】(4 分)

该企业要求在上班时间内(9:00～18:00)禁止内部员工浏览网页(TCP 80 和 TCP 443 端口)，禁止使用 QQ(TCP/UDP 8000 端口以及 UDP 4000)和 MSN(TCP 1863 端口)。另外，在 2015 年 6 月 1 日到 2 日的所有时间内都不允许进行上述操作。除了上述限制外，在任何时间都允许以其他方式访问 Internet。为了防止利用代理服务访问外网，要求对常用的代理服务端口 TCP 8080、TCP 3128 和 TCP 1080 也进行限制。按照要求补充完成(或解释)以下配置命令。

```
Switch-core(config)#time-range TR1
Switch-core(config-time-range)#absolute start 00:00 1 June 2015 end 00:00
3 June 2015
Switch-core(config-time-range)#periodic weekdays start ___(13)___
Switch-core(config-time-range)#exit
…
Switch-core(config)#ip access-list extend internet_limit
Switch-core(config-ext-nacl)#deny tcp 10.1.0.0 0.0.255.255 any eq 80
time-range TR1
Switch-core(config-ext-nacl)#deny tcp 10.1.0.0 0.0.255.255 any eq 443
time-range TR1
//___(14)___
Switch-core(config-ext-nacl)#deny tcp 10.1.0.0 0.0.255.255 any eq 1863
time-range TR1
//___(15)___
Switch-core(config-ext-nacl)#deny tcp 10.1.0.0 0.0.255.255 any eq 8000
time-range TR1
Switch-core(config-ext-nacl)#deny udp 10.1.0.0 0.0.255.255 any eq 8000
time-range TR1
Switch-core(config-ext-nacl)#deny udp 10.1.0.0 0.0.255.255 any eq 4000
time-range TR1
Switch-core(config-ext-nacl)#deny tcp 10.1.0.0 0.0.255.255 any eq 3128
time-range TR1
Switch-core(config-ext-nacl)#deny tcp 10.1.0.0 0.0.255.255 any eq 8080
time-range TR1
Switch-core(config-ext-nacl)#deny tcp 10.1.0.0 0.0.255.255 any eq 1080
time-range TR1
Switch-core(config-ext-nacl)#permit ip any any
Switch-core(config-ext-nacl)#exit
Switch-core(config)#int ___(16)___
Switch-core(config-if)#ip access-group internet_limit out
```

【问题 4】(4 分)

企业要求市场和研发部门不能访问财务部 VLAN 中的数据，但是财务部门作为公司的核心管理部门，又必须能访问到市场和研发部门 VLAN 内的数据。按照要求补充完成(或解

释)以下配置命令。

```
Switch-core(config)#ip access-list extend fi-main
Switch-core(config-ext-nacl)#permit tcp any 10.1.0.0 0.0.255.255 reflect
r-main timeout 120
Switch-core(config-ext-nacl)#permit udp any 10.1.0.0 0.0.255.255 reflect
r-main timeout 200
Switch-core(config-ext-nacl)#permit  icmp  10.1.0.0  0.0.255.255  reflect
r-main timeout 10
Switch-core(config-ext-nacl)#permit ip any any
Switch-core(config-ext-nacl)#exit
Switch-core(config)#int __(17)__
Switch-core(config-if)#ip access-group fi-main in
…
Switch-core(config)#ip access-list extend fi-access-limit
Switch-core(config-ext-nacl)#evaluate r-main
Switch-core(config-ext-nacl)#deny ip any __(18)__
Switch-core(config-ext-nacl)#permit ip any any
Switch-core(config-ext-nacl)#exit
Switch-core(config)#int __(19)__
Switch-core(config-if)#ip access-group fi-access-limit in
Switch-core(config)#int __(20)__
Switch-core(config-if)#ip access-group fi-access-limit in
```

参考答案:

【问题 1】

(1)对数据包进行过滤;

(2)1～99;

(3)源地址;

(4)100～199;

(5)允许;

(6)出口(数据源地址);

(7)入口(数据目的地址)。

【问题 2】

(8)10.1.6.66;

(9)vyt;

(10)in;

(11)10.1.6.33;

(12)10.1.6.0。

【问题 3】

(13)9:00 18:00;

(14)禁止 10.1.0.0/16 的主机在上班时间通过 443 端口访问 Web 服务器;

(15)禁止 10.1.0.0/16 的主机在上班时间通过 1863 端口登录 MSN;

(16)vlan3。





【问题 4】

(17)vlan4；

(18)10.1.4.0 0.0.0.255；

(19)vlan5；

(20)vlan6。

要点解析：

【问题 1】

访问控制列表就是用来在路由技术的网络中，决定这些数据流量是应该被转发还是被丢弃的技术。同时访问控制列表成为实现防火墙的重要手段。

访问控制列表用来限制使用者或设备，控制网络流量，解决拥塞，提高安全性等。在 IP 网络中，可以使用的访问列表有标准访问列表(值为 1～99)、扩展访问列表(标号为 100～199)两种。

同时访问控制列表实际上是一系列的判断语句，这些语句是一种自上而下的逻辑排列的关系。当我们把一个访问控制列表放在接口上面的时候，被过滤的数据包会一个一个地和这些语句的条件进行顺序的比较，以找出符合条件的数据包。当数据包不能符合一条语句的条件，它将向下与下一条语句的条件比较，如果一直不能符合的话，在访问控制列表的最后一项，有一条隐藏的语句，拒绝所有，把数据包丢弃。

对于过滤从同一个源地址到目地址的数据流，在网络中应用标准访问控制列表和应用扩展的访问控制列表的位置是不同的。标准的访问控制列表要尽量放在接近数据流目的的地方，也就是路由器的 in 接口；扩展的访问控制列表要尽量放在接近数据流源的地方，也就是路由器的 out 接口。

【问题 2】

网管要求除了主机 10.1.6.66 能够进行远程 Telnet 到核心设备外，其他用户都不允许进行 Telnet 操作。同时只对员工开放 Web 服务器(10.1.2.20)、FTP 服务器(10.1.2.22)和数据库服务器(10.1.2.21:1521)，研发部除 IP 为 10.1.6.33 的计算机外，都不能访问数据库服务器，按照要求补充完成以下配置命令。

```
access-list 1 permit host 10.1.6.66
line vty 0 4
access-class 1 in
permit tcp host 10.1.6.33 host 10.1.2.21 eq 1521
deny tcp 10.1.6.0 0.0.0.255 host 10.1.2.21 eq 1521
```

【问题 3】

本题主要考查基于时间的 ACL：

第一步，定义一个时间范围。

第二步，在访问表中用 Time-range 引用刚刚定义的时间范围。

定义时间范围又分为两个步骤。

(1)　使用全局 Time-range 命令来正确地指定时间范围。

格式：time-range time-range-name

(2) 使用 Absolute(绝对时间)或者一个或多个 Periodic(循环时间)语句来定义时间范围，每个时间范围只能有一个 Absolute 语句，但它可以有多个 Periodic 语句。所以：

```
periodic weekdays start 9:00 18:00
deny tcp 10.1.0.0 0.0.255.255 any eq 443 time-range TR1//禁止 10.1.0.0/16
的主机在上班时间通过 443 端口访问 Web 服务器
deny tcp 10.1.0.0 0.0.255.255 any eq 1863 time-range TR1//禁止 10.1.0.0/16
的主机通过 1863 端口登录 MSN
int vlan3//配置在核心交换机 vlan3 这边的接口上
```

【问题 4】

两个主机进行通信，需要满足 A 到 B、B 到 A 这两个反向的数据包都不能阻断。

当财务部访问市场部门和研发部门的时候，且当这些部门主机在到达核心交换机的时候，由于普通的 ACL 不具备监测会话状态的能力，就会被 deny ip any 10.1.4.0 0.0.0.255 这条 ACL 阻断，所以不能访问成功。

要实现单方向的访问控制，我们可以在财务部访问市场和研发部门时，在市场和研发部门的 ACL 临时生成一个反向的 ACL 条目。

int vlan4//反向的 ACL 应用在财务部所在 VLAN4 的 in 接口上

deny ip any 10.1.4.0 0.0.0.255

int vlan5

int vlan6

试题 7 (2015 年下半年下午试题四)

【说明】

某公司网络拓扑结构图如图 9.10 所示。公司内部的用户使用私有地址段 192.168.1.0/24。

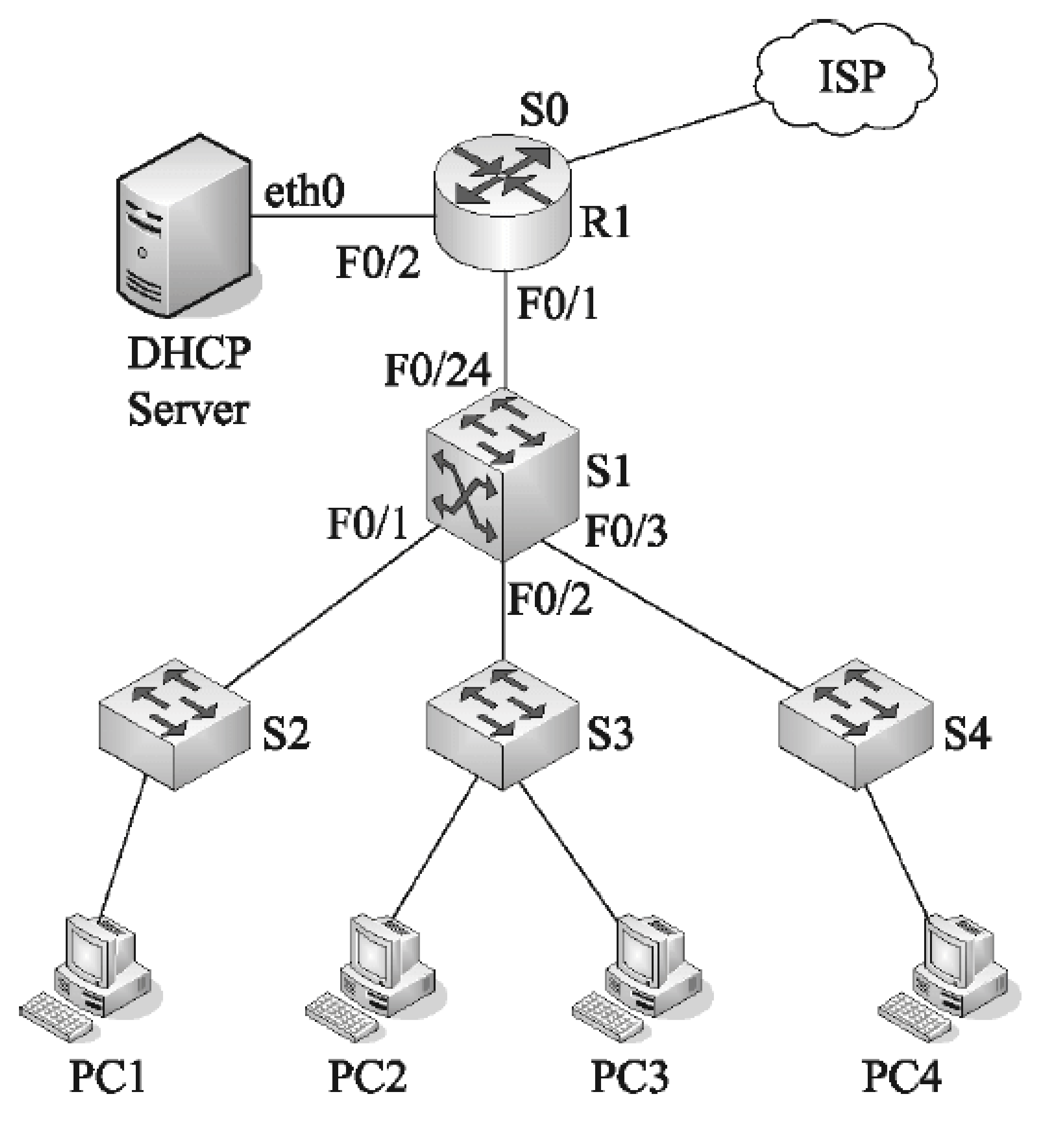


图 9.10 网络拓扑结构图

【问题 1】(2 分)

为了节省 IP 地址，在接口地址上均使用 30 位地址掩码，请补充表 9.9 中的空白。

表 9.9　设备接口与地址

设　备	接　口	IP 地址	设　备	接　口	IP 地址
S1	F0/24	192.168.1.253	R1	F0/1	(1)
DHCPServer	Eth0	192.168.1.249		F0/2	(2)

【问题 2】(9 分)

将公司内部用户按照部门分别划分在 3 个 vlan 中：vlan 10、vlan 20 和 vlan 30。均连接在交换机 S1 上，并通过 S1 实现 vlan 间通信，所有内网主机均采用 DHCP 获取 IP 地址。按照要求补充完成(或解释)以下配置命令。

```
Switch>en
Switch#  (3)
Switch(config)#hostname  (4)
S1(config)#interface fastEthernet 0/1
S1(config-if)#  (5)  mode trunk
S1(config)#interface vlan 10      //  (6)
S1(config-if)#ip address 192.168.1.206  255.255.255.240
S1(config-if)#no shutdown
S1(config-if)#ip helper-address  (7)
S1(config-if)#  (8)
S1(config)#
…
S1(config)#router  (9)
S1(config-router)#version  (10)
S1(config-router)#network 192.168.1.192
S1(config-router)#network 192.168.1.208
S1(config-router)#network 192.168.1.224
S1(config-router)#  (11)
S1#
```

【问题 3】(2 分)

在 S1 上将 F0/1 接口配置为 trunk 模式时，出现了以下提示：

```
Command rejected: An interface whose trunk encapsulation is "Auto" cannot
be configured to "trunk" mode.
```

应采取 (12) 方法解决该问题。

(12) A. 在该接口上使用 no shutdown 命令后再使用该命令
B. 在该接口上启用二层功后再能使用该命令
C. 重新启动交换机后再使用该命令
D. 将该接口配置为 access 模式后再使用该命令

【问题 4】(2 分)

在 S1 上配置的三个 SVI 接口地址分别处在 192.168.1.192、192.168.1.208 和 192.168.1.224 网段，它们的子网掩码是 (13) 。

参考答案：

【问题 1】

(1)192.168.1.254；(2)192.168.1.250。

【问题 2】

(3)config terminal；(4)S1；(5)switchport；(6)进入 vlan10 中；(7)192.168.1.249；(8)exit；(9)rip；(10)2；(11)end。

【问题 3】

(12)D。

【问题 4】

(13)255.255.255.240。

要点解析：

【问题 1】

为了节省 IP 地址，在接口地址上均使用 30 位地址掩码，R1 的 F0/1 和 S1 的 F0/24 在同一网络中，那么现在 S1 的 F0/24 地址是 192.168.1.253，子网掩码是 255.255.255.252，那么这个地址所在的可用主机地址范围是 192.168.1.253～192.168.1.254。那么 R1 的 F0/1 就是 192.168.1.254。

同理 R1 的 F0/2 和 DHCP 的 eth0 处于同一网络，所以 R1 的 F0/2 的地址是 192.168.1.250。

【问题 2】

(3)Switch#config terminal //进入全局配置模式

(4)Switch(config)#hostname S1 //将交换机命名为 S1

(5)S1(config-if)switchport mode trunk //将端口封装为 trunk 模式

(6)S1(config-if)#interface vlan 10//进入 vlan10

(7)S1(config-if)#ip helper-address 192.168.1.249//指定 DHCP 服务器的地址，表示通过 Ethernet0 向该服务器发送 DHCP 请求包

(8)S1(config-if)#exit//退出接口子模式

(9)S1(config)#route rip//开启 RIP

(10)S1(config-router)#version 2//指定版本为 2，支持可变长子网掩码

(11)S1(config-router)#end//退出到特权模式

【问题 3】

在 S1 上将 F0/1 接口配置为 trunk 模式时，出现了以下提示：

Command rejected：An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode.

应采取将该接口配置为 access 模式后再使用该命令的方法解决该问题。

【问题 4】

采用三层交换机的路由模块为 VLAN 之间做路由也是非常普遍的。由于三层交换机的路由模块和交换模块直接通过交换机的背板总线连接，所以不需要使用干道技术。只需要在三层交换机的路由模块上定义与 VLAN 数量相当的逻辑接口，并让这些接口和 VLAN 对应，为这些接口分配 IP 地址就可以了。SVI 交换机虚拟接口实现不同 VLAN 间通信的问题，



每个 SVI 要和各个 VLAN 属于同一网络中。所以子网掩码是 255.255.255.240。

试题 8 （2015 年上半年下午试题四）

【说明】

某企业的网络拓扑结构如图 9.11 所示。

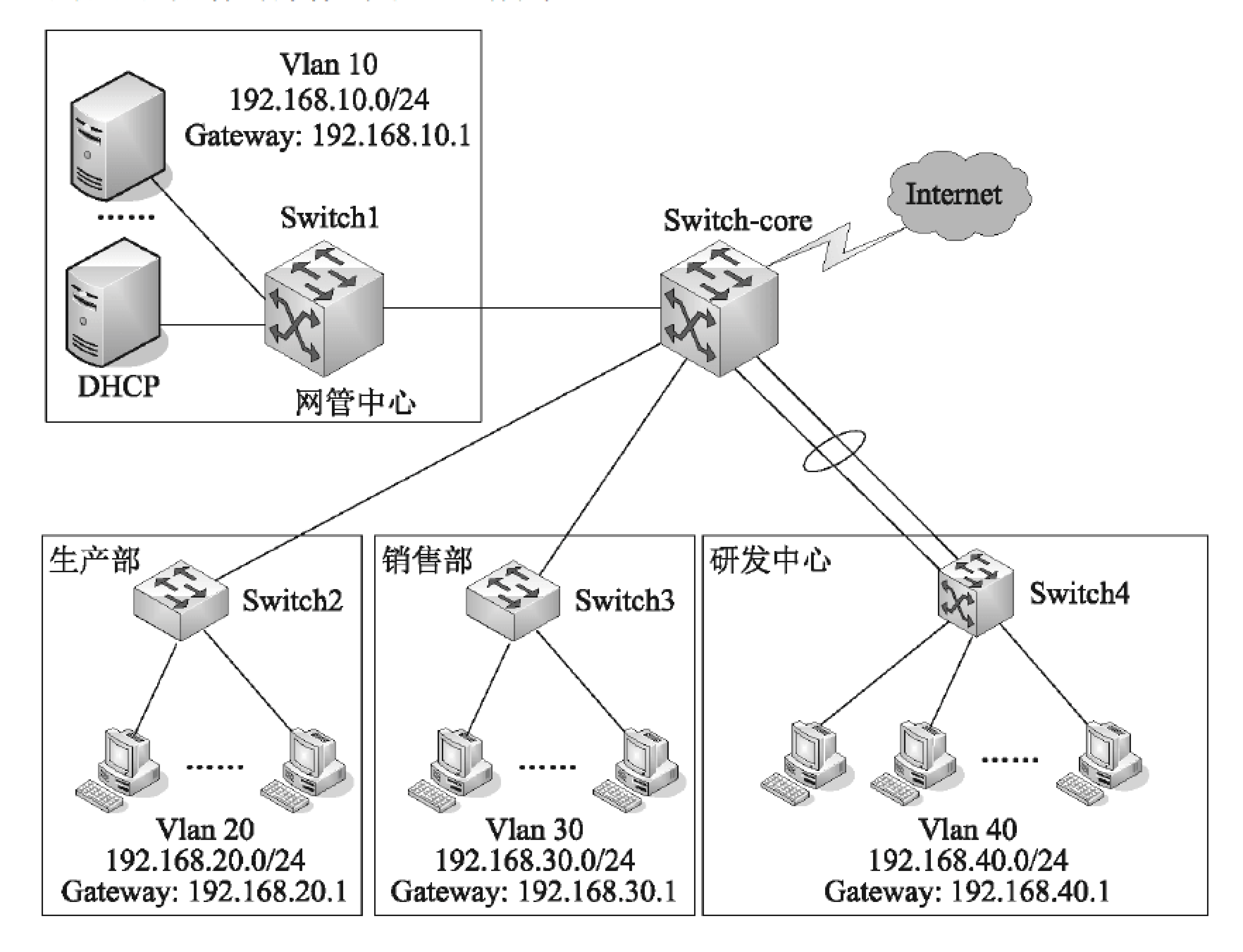


图 9.11　某企业网络拓扑结构

由于该企业路由设备数量较少，为提高路由效率，要求为该企业构建基于静态路由的多层安全交换网络。根据要求创建 4 个 VLAN 分别属于网管中心、生产部、销售部以及研发中心，各部门的 VLAN 号及 IP 地址规划如图 9.11 所示。该企业网采用三层交换机 Switch-core 为核心交换机，Switch-core 与网管中心交换机 Switch1 和研发中心交换机 Switch4 采用三层连接，Switch-core 与生产部交换机 Switch2 及销售部交换机 Switch3 采用二层互连。

各交换机之间的连接以及接口 IP 地址如表 9.10 所示。

表 9.10　各交换机之间的连接以及接口 IP 地址表

上联端口				下联端口			
交换机	端口	描述	IP 地址	交换机	端口	描述	IP 地址
Switch-core	G0/1	scsw-g1/1		Switch2	G1/1	core-g0/1	
	G0/2	scsw-g0/1	192.168.101.1/24	Switch1	G0/1	core-g0/2	192.168.101.2/24
	F0/1	yfsw-f0/1	192.168.102.1/24	Switch4	F0/1	core-f0/1	192.168.102.2/24
	F0/2	yfsw-f0/2			F0/2	core-f0/2	
	F0/3	yfsw-f0/3			F0/3	core-f0/3	
	F0/4	yfsw-f0/4			F0/4	core-f0/4	
	F0/5	xssw-f0/1		Switch3	F0/1	core-f0/5	

【问题1】(4分)

随着企业网络的不断发展，研发中心的上网计算机数急剧增加，在高峰时段研发中心和核心交换机之间的网络流量非常大，在不对网络进行大的升级改造的前提下，网管人员采用了以太信道(或端口聚合)技术来增加带宽，同时也起到了__(1)__和__(2)__的作用，保证了研发中心网络的稳定性和安全性。

在两台交换机之间是否形成以太信道，可以用协议自动协商。目前有两种协商协议：一种是__(3)__，是Cisco私有的协议；另一种是__(4)__，是基于IEEE 802.3ad标准的协议。

(3)、(4)备选答案：

A. 端口聚合协议(PAgP)

B. 多生成树协议(MSTP)

C. 链路聚合控制协议(LACP)

【问题2】(7分)

核心交换机Switch-core与网管中心交换机Switch1通过静态路由进行连接。根据需求，完成或解释Switch-core与Switch1的部分配置命令。

(1) 配置核心交换机Switch-core

```
Switch-core#config terminal
Switch-core(config)#interface gigabitEthernet 0/2
Switch-core(config-if)#description wgsw-g0/1    //__(5)__
Switch-core(config-if)#no switchport          //__(6)__
Switch-core(config-if)#ip address __(7)__
Switch-core(config-if)#no shutdown
Switch-core(config)#ip route 192.168.10.0 255.255.255.0 192.168.101.2
Switch-core(config)#exit
...
```

(2) 配置网管中心交换机Switch1

```
Switch1#config terminal
Switch1(config)#no ip domain lookup            //__(8)__
Switch1(config)#interface gigabitEthernet 0/1
Switch1(config-if)#description core-g0/2
Switch1(config-if)#no switchport
Switch1(config-if)#ip address __(9)__
Switch1(config-if)#exit
Switch1(config)#vlan 10
Switch1(config-vlan)#name wg10
Switch1(config-vlan)#exit
Switch1(config)#interface vlan 10              //创建 VLAN10
Switch1(config-if)#ip address __(10)__
Switch1(config-if)#exit
Switch1(config)#interface range f0/2-20
Switch1(config-if-range)#switchport mode access    //设置端口为access模式
Switch1(config-if-range)#switchport access __(11)__//设置端口所属的VLAN
Switch1(config-if-range)#no shutdown
Switch1(config-if-range)#exit
Switch1(config)#ip route 192.168.20.0 255.255.255.0 192.168.101.1
Switch1(config)#ip route 192.168.30.0 255.255.255.0 192.168.101.1
...
```



【问题 3】(7 分)

为确保研发中心网络的稳定性，在现有条件下尽量保证带宽，要求实现核心交换机 Switch-core 与研发中心交换机 Switch4 的三层端口聚合，然后通过静态路由进行连接。根据需求，完成或解释以下配置命令。

(1) 继续配置核心交换机 Switch-core

```
Switch-core#config terminal
Switch-core(config)#interface port-channel 10        //__(12)__
Switch-core(config-if)#no switchport
Switch-core(config-if)#ip address__(13)__
Switch-core(config-if)#no shutdown
Switch-core(config-if)#exit
Switch-core(config)#interface range fastEthernet0/1-4  //选择配置的物理接口
Switch-core(config-if-range)#no switchport
Switch-core(config-if-range)#no ip address   //确保该物理接口没有指定的 IP 地址
Switch-core(config-if-range)#switchport      //改变该端口为 2 层接口
Switch-core(config-if-range)#channel-group 10 mode on    //__(14)__
Switch-core(config-if-range)#no shutdown
Switch-core(config-if-range)#exit
Switch-core(config)#ip route 192.168.40.0 255.255.255.0 192.168.102.2
…
```

(2) 配置研发中心交换机 Switch4

```
Switch4#config terminal
Switch4(config)#interface port-channel 10
Switch4(config-if)#no switchport
Switch4(config-if)#ip address__(15)__
Switch4(config-if)#no shutdown
Switch4(config-if)#exit
Switch4(config)#interface range fastEthernet0/1-4      //选择配置的物理接口
Switch4(config-if-range)#no switchport
Switch4(config-if-range)#no ip address
…
Switch4(config-if-range)#no shutdown
Switch4(config-if-range)#exit
Switch4(config)#__(16)__                    //配置默认路由
Switch4(config)#vlan 40
Switch4(config-vlan)#name yfl0
Switch4(config-vlan)#exit
Switch4(config)#__(17)__                    //开启该交换机的三层路由功能
Switch4(config)#interface vlan 40
Switch4(config-if)#ip address 192.168.40.1 255.255.255.0
Switch4(config-if)#exit
Switch4(config)#interface range fastEthernet0/5-20
Switch4(config-if-range)#switchport mode access
…
Switch4(config-if-range)#__(18)__                //退回到特权模式
Switch4#
…
```

【问题 4】(2 分)

为了保障局域网用户的网络安全，防范欺骗攻击，以生产部交换机 Switch2 为例，配置 DHCP 侦听。根据需求完成或解释 Switch2 的部分配置命令。

```
Switch2#config terminal
Switch2(config)#ip dhcp snooping        //  (19)
Switch2(config)#ip dhcp snooping vlan 20
Switch2(config)#interface gigabitEthernet1/1
Switch2(config-if)#ip dhcp snooping trust   //  (20)
Switch2(config-if)#exit
…
```

参考答案：

【问题 1】

(1)负载均衡；(2)冗余备份；(3)A；(4)C。

【问题 2】

(5)配置接口描述；(6)设置为路由接口；(7)192.168.101.1　255.255.255.0；(8)禁止 DNS 查询；(9)192.168.101.2　255.255.255.0；(10)192.168.10.1　255.255.255.0；(11)vlan 10。

【问题 3】

(12)进入编号为 10 的通道接口；(13)192.168.102.1　255.255.255.0；(14)配置通道组 10 的模式为启动；(15)192.168.102.2　255.255.255.0；(16)ip route 0.0.0.0　0.0.0.0　192.168.102.1；(17)ip routing；(18)end。

【问题 4】

(19)启动 DCHP 监听功能；(20)设置端口为信任端口。

要点解析：

【问题 1】

以太通道可以增加带宽，同时也可以起到负载均衡和冗余备份的作用。

Cisco 的以太通道的协议是 PAgP，IEEE 802.3ad 的以太通道协议是 LACP。

【问题 2】

(5)Switch-core(config-if)#description wgsw-g0/1　　// 配置端口描述

(6)Switch-core(config-if)#no switchport　　// 设置为路由(三层)接口

(7)Switch-core(config-if)#ip address 192.168.101.1　255.255.255.0

(8)Switch1(config)#no ip domain lookup　　// 禁止 DNS 查询

(9)Switch1(config-if)#ip address 192.168.101.2 255.255.255.0 //通过表中可得出 Switch1 的 g0/2 的 IP 地址

(10)Switch1(config-if)#ip address 192.168.10.1 255.255.255.0
//通过图中网管主机的网关地址可得出

(11)Switch1(config-if-range)#switchport access　vlan 10　//设置端口所属的 VLAN

【问题 3】

(12)Switch-core(config)#interface port-channel 10　　// 进入编号为 10 的以太网通道接口

(13)Switch-core(config-if)#ip address 192.168.102.1 255.255.255.0
//为该接口分配 IP 地址和子网掩码



(14)Switch-core(config-if-range)#channel-group 10 mode on
　　//分配接口并指定为 PAgP 模式
(15)Switch4(config-if)#ip address 192.168.102.2 255.255.255.0
　　//为该接口分配 IP 地址和子网掩码
(16)Switch4(config)#ip route 0.0.0.0 0.0.0.0 192.168.102.1　　//配置默认路由
(17)Switch4(config)# ip routing　　//开启该交换机的三层路由功能
(18)Switch4(config-if-range)#end　　//退回到特权模式

【问题 4】

DHCP Snooping 技术是 DHCP 安全特性，通过建立和维护 DHCP Snooping 绑定表过滤不可信任的 DHCP 信息，这些信息是指来自不信任区域的 DHCP 信息。DHCP Snooping 绑定表包含不信任区域的用户 MAC 地址、IP 地址、租用期、VLAN-ID 接口等信息。

当交换机开启了 DHCP-Snooping 后，会对 DHCP 报文进行侦听，并可以从接收到的 DHCP Request 或 DHCP Ack 报文中提取并记录 IP 地址和 MAC 地址信息。另外，DHCP-Snooping 允许将某个物理端口设置为信任端口或不信任端口。信任端口可以正常接收并转发 DHCP Offer 报文，而不信任端口会将接收到的 DHCP Offer 报文丢弃。这样，可以完成交换机对假冒 DHCP Server 的屏蔽作用，确保客户端从合法的 DHCP Server 获取 IP 地址。

9.4 强化训练

9.4.1 综合知识试题

试题 1 (2014 年下半年试题 11 和试题 12)

思科路由器的内存体系由多种存储设备组成，其中用来存放 BIOS 引导程序的是__(11)__，运行时活动配置文件存放在__(12)__中。

(11) A. FLASH　B. ROM　C. NVRAM　D. DRAM
(12) A. FLASH　B. ROM　C. NVRAM　D. DRAM

试题 2 (2014 年下半年试题 46)

把交换机由特权模式转换到全局配置模式使用的命令是__(46)__。

(46) A. interface f0/1　B. config terminal　C. enable　D. no shutdown

试题 3 (2014 年下半年试题 48)

利用扩展 ACL 禁止用户通过 Telnet 访问子网 202.112.111.0/24 的命令是__(48)__。

(48) A. access-list 110 deny telnet any 202.112.111.0 0.0.0.255 eq 23
　B. access- list 110 deny udp any 202.112.111.0 eq telnet
　C. access-list 110 deny tcp any 202.112.111.0 0.0.0.255.eq 23
　D. access-list 10 deny tcp any 202.112.111.0 255.255.255.0 eq 23

试题 4 (2014 年下半年试题 57)

每一个访问控制列表(ACL)最后都隐含着一条__(57)__语句。

(57) A. deny any B. deny all C. permit any D. permit all

试题 5 (2014 年下半年试题 58)

以下关于访问控制列表的论述中，错误的是__(58)__。

(58) A. 访问控制列表要在路由器全局模式下配置

B. 具有严格限制条件的语句应放在访问控制列表的最后

C. 每一个有效的访问控制列表至少应包含一条允许语句

D. 访问控制列表不能过滤由路由器自己产生的数据

试题 6 (2014 年上半年试题 11 和试题 12)

路由器连接帧中继网络的接口是__(11)__，连接双绞线以太网的接口是__(12)__。

(11)、(12)A. AUI B. RJ-45 C. Console D. Serial

试题 7 (2014 年上半年试题 28 和试题 29)

网络配置如图 9.12 所示，在路由器 Router 中配置网络 1 访问 DNS 服务器的命令是__(28)__。网络 1 访问 Internet 的默认路由命令是__(29)__。

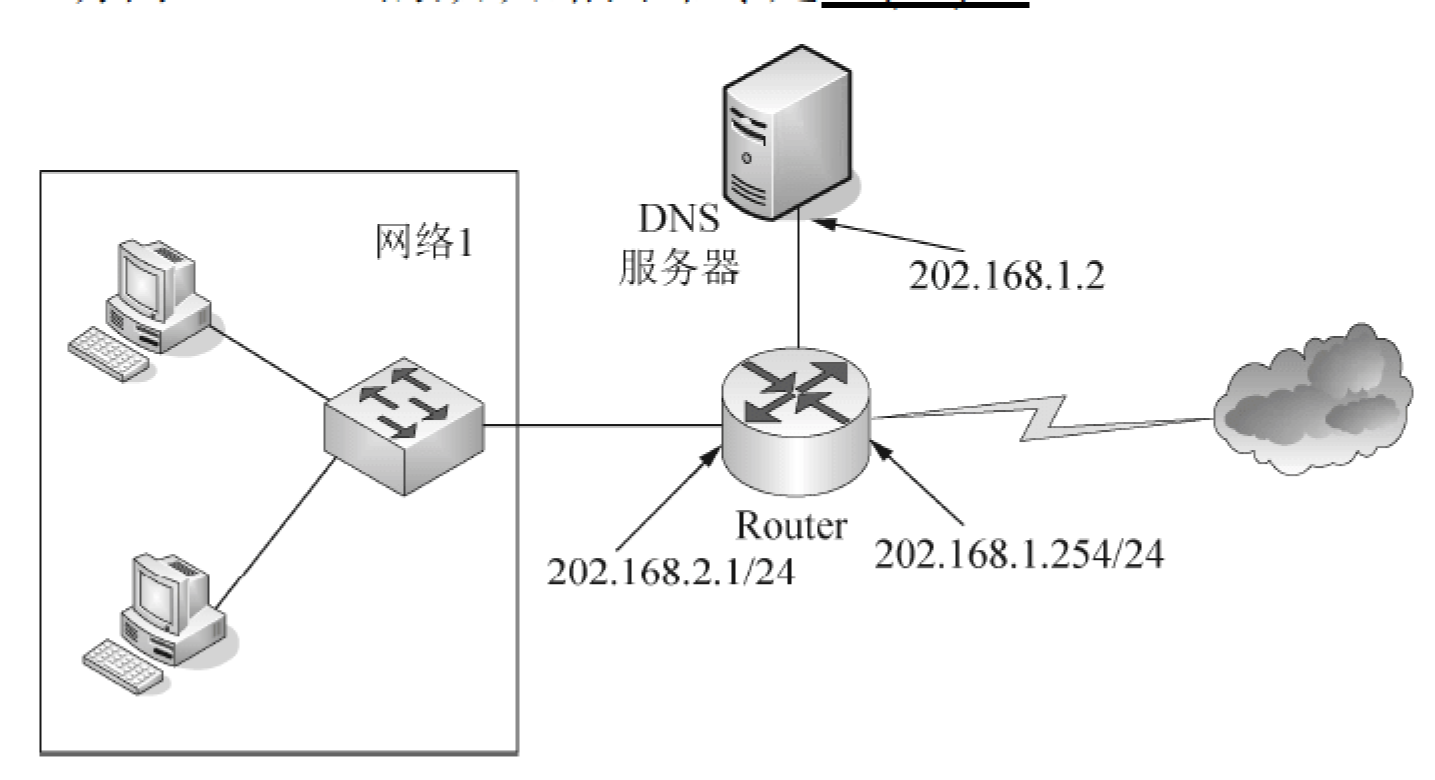


图 9.12 网络配置

(28) A. ip route 202.168.1.2 255.255.255.0 202.168.1.2

B. ip route 202.168.1.2 255.255.255.255 202.168.1.2

C. ip route 0.0.0.0 0.0.0.0 202.168.1.253

D. ip route 255.255.255.255 0.0.0.0 202.168.1.254

(29) A. ip route 202.168.1.2 255.255.255.0 202.168.1.2

B. ip route 202.168.1.2 255.255.255.255 202.168.1.2

C. ip route 0.0.0.0 0.0.0.0 202.168.1.253

D. ip route 255.255.255.255 0.0.0.0 202.168.1.254

9.4.2 案例分析试题

试题 1 (2014 年下半年下午试题三)

【说明】

某企业的网络结构如图 9.13 所示。





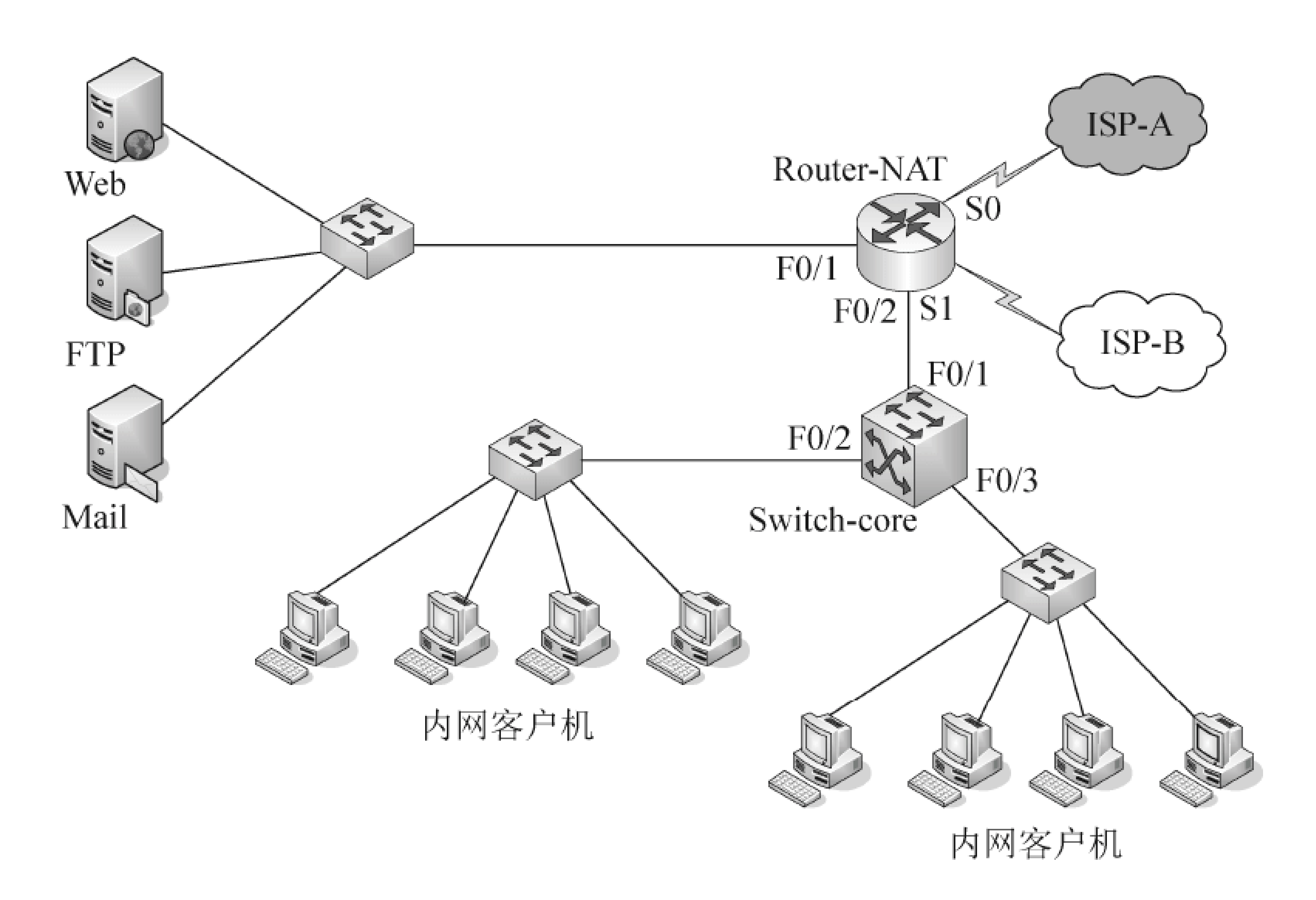


图 9.13　企业网络拓扑结构

按照网络拓扑结构为该企业网络进行网络地址配置，地址分配如表 9.11 所示。

表 9.11　网络地址分配表

设　备	地　址
Router-NAT	F0/1: 192.168.1.1/24 S0: 61.192.93.100/24 S1: 202.102.100.100/24
Web 服务器	192.168.1.100
ISP-A	61.192.93.200/24
ISP-B	202.102.100.200/24
ISP-A 地址池	61.192.93.100～61.192.93.102
ISP-B 地址池	202.102.100.100～202.102.100.102

【问题 1】(4 分)

企业网络中使用私有地址，如果内网用户要访问互联网，一般用__(1)__技术将私有网路地址转换为公网地址。在用该技术时，往往是用__(2)__技术指定允许转换的内部主机地址范围。一般来说，企业内服务器需要被外部用户访问，就必须对其做地址变换，内部服务器映射的公共地址不能随意更换，需要使用__(3)__技术。但是对于企业内部用户来讲，使用一一映射的技术为每个员工配置一个地址很不现实，一般使用__(4)__技术以提高管理效率。

【问题 2】(7 分)

一般企业用户可能存在于任何一家运营商的网络中，为了确保每个运营商网络中的客户都可以高效地访问本企业所提供的网络服务，企业有必要同时接入多个运营商网络，根据企业网络的拓扑图和网络地址规划表，实现该企业出口的双线接入。

首先，为内网用户配置 NAT 转换，其中以 61.192.93.0/24 代表 ISP-A 所有网段；其次为外网用户访问内网服务器配置 NAT 转换。根据需求，完成以下 Route-NAT 的有关配置命令。

```
Route-Switch(config)#access-list 100 permit ip any 61.192.93.0 0.0.0.255
//定义到达 ISP-A 所有网段的 ACL
Route-Switch(config)#access-list 101__(5)__ip any 61.192.93.0 0.0.0.255
Route-Switch(config)#access-list 101__(6)__
//定义到达 ISP-B 所有网段的 ACL
Route-Switch(config)#ip nat pool ISP-A__(7)__netmask 255.255.255.0
//定义访问 ISP-A 的合法地址池
Route-Switch(config)#ip nat pool ISP-B__(8)__netmask 255.255.255.0
//定义访问 ISP-B 的合法地址池
Route-Switch(config)#ip nat inside source list100 pool ISP-A overload
Route-Switch(confg)#ip nat inside source__(9)__
//为内网用户实现区分目标运营商网络进行匹配的 NAT 转换
Route-Switch(config)#ip nat inside source static tcp__(10)__extendable
//为内网 Web 服务器配置 ISP-A 的静态 NAT 转换
Route-Switch(config)#ip nat inside source static tcp__(11)__extendable
//为内网 Web 服务器配置 ISP-B 的静态 NAT 转换
```

【问题 3】(6 分)

在路由器的内部和外部接口启用 NAT，同时为了确保内网可以访问外部网络，在出口设备配置静态路由，根据需求，完成(或解释)Route-NAT 的部分配置命令。

```
Route-Switch(config)#int S0
Route-Switch(config)#__(12)__//指定 NAT 的外部转换接口
Route-Switch(config)#int S1
Route-Switch(config)#__(13)__//指定 NAT 的外部转换接口
Route-Switch(config)#int f0/1
Route-Switch(config)#__(14)__//指定 NAT 的内部转换接口
Route-Switch(config)#__(15)__//配置到达 ISP-A 的流量从 S0 口转发
Route-Switch(config)#__(16)__//配置默认路由指定从 S1 口转发
Route-Switch(config)#ip route 0.0.0.0 0.0.0.0 S0 120   //__(17)__
```

【问题 4】(3 分)

QoS(服务质量)主要用来解决网络延迟和阻塞等问题，它主要有三种工作模式，分别为__(18)__模型、Integrated service(集成服务)模型及__(19)__模型，其中使用比较普遍的方式是__(20)__模型。

试题 2 (2014 年下半年下午试题四)

【说明】

某公司网络拓扑结构如图 9.14 所示。公司内部用 C 类私有 IP 地址，其中公司两个部门分别处于 VLAN10 和 VLAN20，VLAN10 采用 192.168.10.0/24 网段，VLAN20 采用 192.168.20.0/24 网段，每段最后一个地址作为网关地址。



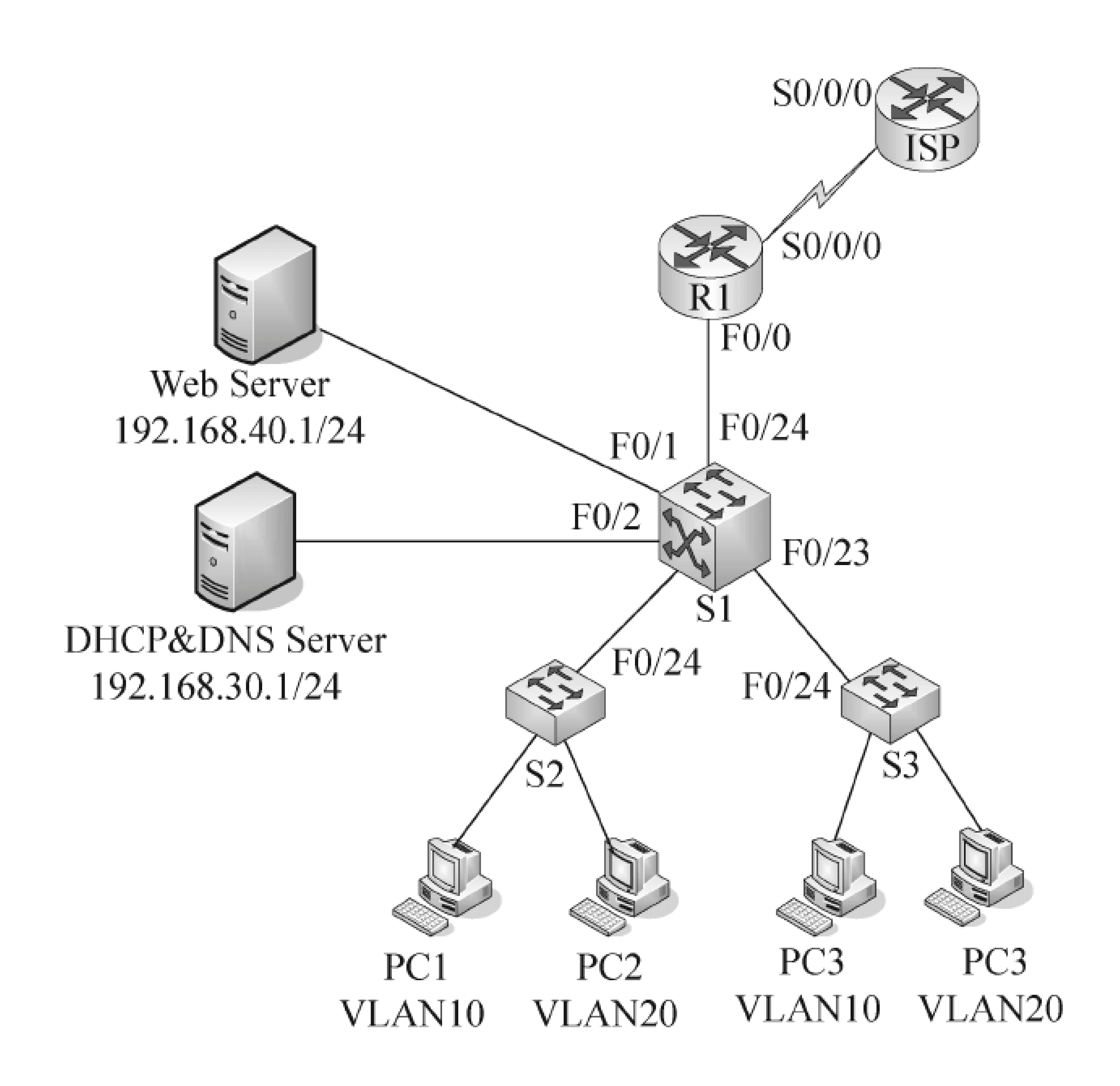


图 9.14　某公司网络拓扑结构

【问题 1】(10 分)

公司使用规划 VTP 协议规划 VLAN，三层交换机 S1 为 VTP Sever，其他交换机为 VTP Client，并通过 S1 实现 VLAN 间通信。请根据网络拓扑和需求说明，完成交换机 S1 和 S2 的配置。

```
S1 >enable
S1 #configure terminal
S1 (config)#vtp mode  (1)
S1 (config)#vtp domain shx
S1 (config)#vtp password shx
S1 (config)#vlan 10
S1 (config-vlar)#exit
S1 (config)#vlan 20

S1 (config-vku)#exit
S1 (config)#interface vlan 10
S1 (config-if)#ip address  (2)    (3)
S1 (config-vlar)#exit
S1 (config)#interface vlan 20
S1 address 192.16820254 255.255-255.0
S1 (config-if)#exit
S1 (config)#interface  (4)   fastethernet 0/22-23
S1 (config-if-range)#switchport mode access
S1 (config-if-range)#switchport mode  (5)

S1 (config-if-range)#exit
S1 (config)#interface fastethernet 0/1
S1 (config-if)#  (6)  //关闭二层功能
```

```
S1 add 192.168.40.254 255.255.255.0
S1 (config-if)#exit

S1 (config)# __(7)__ __(8)__ //开启路由功能
S1 (config)#

S2 >enable
S2 #configure terminal
S2 (config)#vtp mode __(9)__
S2 (config)#vtp domain shx
S2 (config)#vtp password shx
S2 (config)#interface fastethernet 0/24
S2 (config-if)#switchport mode __(10)__ / / 设定接口模式
S2 (config-if)#end
S2 #
```

【问题 2】(5 分)

公司申请了 202.165.200.0/29 地址段，使用 NAT-PT 为用户提供 Internet 访问，外部全局地址为 202.165.200.1，Web 服务器使用的外部映射地址为 202.165.200.3。请根据网络拓扑和需求说明，完成路由器 R1 的配置。

```
R1>enable
R1#config terminal
R1 (config)# access-list1 __(11)__ 192.168.10.0  255.255.255.0
…
R1(config)#interface serial 0/0/0
R1 (config-if)#ip address 202.165.200.1 255.255.255.248
R1 (config-if)#no shutdown
R1 (config-if)#clock rate 4000000
R1 (config-if)#interface fastethernet 0/0
R1 (config-if)#ip address 192.168.50.254 255.255.255.0
R1 (config-if)#no shutdown
R1 (config-if)#exit
R1 (config)#ip nat inside source __(12)__ 1 interface S0/0/0 Overload
…
R1 (config)#ip nat inside source static __(13)__ 202.165.200.3
R1 (config)#interface fastethernet 0/0
R1 (config-if)#ip nat __(14)__
R1 (config-if)#interface serial 0/0/0
R1 (config-if)#ip nat __(15)__
R1 (config-if)#end
R1 #
```

试题 3 (2014 年上半年下午试题四)

【说明】

某企业总部设立在 A 地，在 B 地有分支机构，分支机构和总部需要在网络上进行频繁的数据传输，该企业采用 IPSec VPN 虚拟专用技术实现分支机构和总部直接的安全、快捷、经济的跨区域网络连接。

该企业网络拓扑结构如图 9.15 所示。





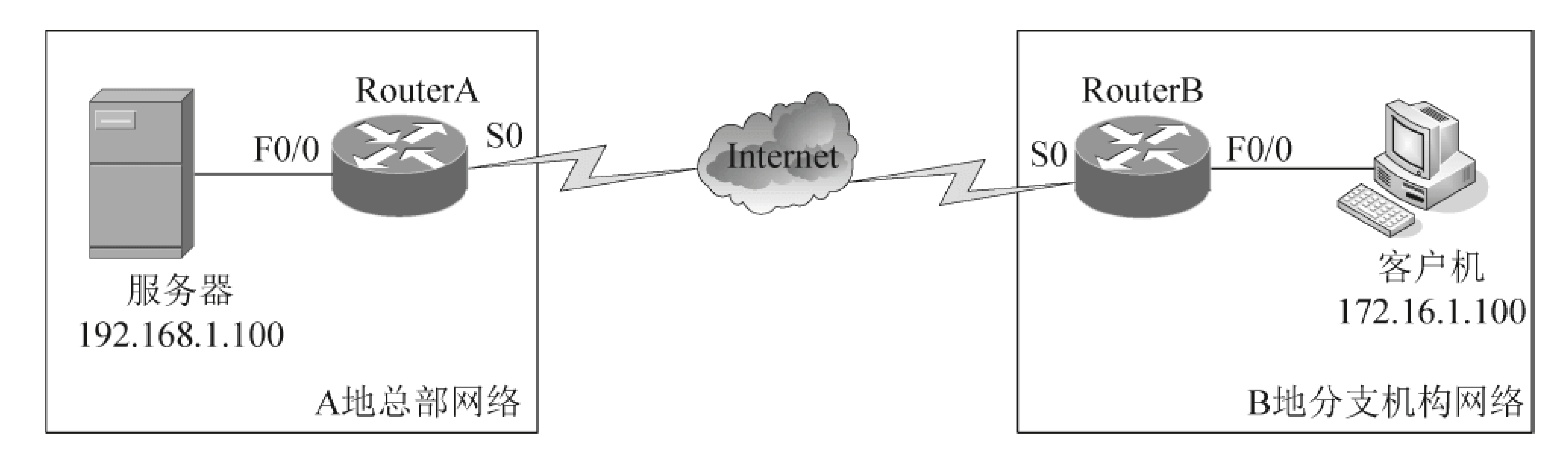


图 9.15　企业网络拓扑结构

该企业的网络地址规划及配置如表 9.12 所示。

表 9.12　网络规划地址配置表

设　备	IP 地址	设　备	IP 地址
RouterA	F0/0: 172.16.1.1/24 S0:202.102.100.1/30	RouterB	F0/0:192.168.1.1/24 S0:202.102.100.2/30
总部服务器	192.168.1.100/24	分支机构客户端	172.16.1.100/24

【问题 1】(7 分)

为了完成对 RouterA 和 RouterB 远程连接管理，以 RouterA 为例，完成初始化路由器，并配置 RouterA 的远程管理地址(192.168.1.20)，同时开启 RouterA 的 Telent 功能并设置全局模式访问密码，请补充下列配置命令。

```
RouterA>enable
RouterA#configure terminal
RouterA(config)#interface f0/0  //进入 F0/0 的(1)子模式
RouterA(config-if)#ip addr __(2)__ //为 F0/0 接口配置 IP 地址
RouterA(config-if)#no shut  //__(3)__F0/0 接口，默认所有路由器的接口都为 down 状态
RouterA(config-if)#inter__(4)__//进入 loopback0 的接口配置子模式
RouterA(config-if)#ip addr __(5)__//为 loopback0 接口配置 IP 地址
RouterA(config)#__(6)__//进入虚拟接口 0-4 的配置子模式
RouterA(config-line)#password abc001//配置 vty 口令为"abc001"
RouterA(config)#enable password abc001//配置全局配置模式的明文密码为"abc001"
RouterA(config)#enable __(7)__ abc001//配置全局配置模式的密文密码为"abc001"
```

【问题 2】(5 分)

VPN 是建立在两个局域网出口之间的隧道链接，所以两个 VPN 设备必须能够满足内外访问互联网的要求，以及需要配置 NAT，按照题目要求以 RouterA 为例，请补充完成下列配置命令。

```
RouterA(config)#access-list 101 __(8)__ ip 192.168.1.0 0.0.0.255 172.16.1.00.0.0255
RouterA(config)#access-list 101 __(9)__ ip 192.168.1.0 0.0.0.255 any //定义需要被 NAT 的数据流
RouterA(config)#ip nat inside sourcelist 101 interface __(10)__overload //定义 NAT 转换关系
RouterA(config)#int __(11)__
RouterA(config-if)#ip nat inside
RouterA(config)#int __(12)__
```

```
RouterA(config-if)#ip nat outside //定义 NAT 的内部和外部接口
```

【问题 3】(4 分)

配置 IPSec VPN 时，要注意隧道两端的设备配置参数必须对应匹配，否则 VPN 配置将会失败。以 RouterB 为例，配置 IPSec VPN，请完成相关配置命令。

```
RouterB(config)#access-list 102 permit ip __(13)__ //定义需要经过 VPN 加密传输的数据流
RouterB(config)#crypto isakmp __(14)__ //启用 ISAKMP(IKE)
RouterB(config)#crypto isakmp policy 10
RouterB(config-isakmp)#authentication pre-share
RouterB(config-isakmp)#encryption des
RouterB(config-isakmp)#hash md5
RouterB(config-isakmp)#group 2
RouterB(config)#crypto isakmp identity address
RouterB(config)#crypto isakmp key abc001 address __(15)__ //指定共享密匙和对端设备地址
RouterB(config)#crypto ipsec transform-set ccie esp-des esp-md5-hmac
RouterB(cfg-crypto-trans)#model tunnel
RouterB(config)#crypto map abc001 10 ipsec-isakmp
RouterB(config)#int __(16)__
RouterB(config)-if)#crypto map abc001 //在外部接口上应用加密图
```

【问题 4】(4 分)

根据题目要求，企业分支机构与总部之间采用 IPSec VPN 技术互连，IPSec(IP Security)是 IETE 为保证在 Internet 上传输数据的安全性、保密性而制定的框架协议。该协议使用在__(17)__层，用于保证和认证用户 IP 数据包。

IPSec VPN 可使用的模式有两种，其中__(18)__模式的安全性较强，__(19)__模式的安全性较弱。IPSec 主要由 AH/ESP 和 IKE 组成。在使用 IKE 协议时，需要定义 IKE 协商策略。该策略由__(20)__进行定义。

9.4.3 综合知识试题参考答案

【试题 1】答　案：(11)A；(12)C。

解　析：Flash 内存即 Flash Memory，全名叫 Flash EEPROM Memory，又名闪存，是一种长寿命的非易失性(在断电情况下仍能保持所存储的数据信息)的存储器。由于其断电时仍能保存数据，闪存通常被用来保存设置信息，如在电脑的 BIOS(基本输入输出程序)。

NVRAM 非易失性随机访问存储器 (Non-Volatile Random Access Memory)，是指断电后仍能保持数据的一种 RAM。Cisco Router 启动时的关键值就存储在 NVRAM。

【试题 2】答　案：(46)B。

解　析：交换机和路由器的模式大体可分为四层：用户模式→特权模式→全局配置模式→子配置模式。进入某模式时，需要逐层进入，如表 9.13 所示。

表 9.13　模式切换命令表

要　求	举　例
进入用户模式	—
进入特权模式	Switch>enable Switch #
进入全局配置模式	Switch #configure terminal Switch (config)#

【试题 3】答　案：(48)C。

解　析：本题考查 ACL 配置命令的使用。

首先，利用扩展 ACL 可排除 A 和 D 选项；其次 B 选项中使用了 UDP，Telnet 是基于 TCP 协议的，所以 B 选项错误。

【试题 4】答　案：(57)A。

解　析：访问控制列表(ACL)是应用在路由器接口上的指令列表。这些指令列表用来告诉路由器哪些数据包可以收、哪些数据包需要拒绝。至于数据包是被接收还是拒绝，可以由类似于源地址、目的地址、端口号等的特定指示条件来判断决定。

将数据包和访问列表进行比较时应遵循的重要规则：

(1) 数据包到来，则按顺序比较访问列表的每一行。

(2) 按顺序比较访问列表的各行，直到找到匹配的一行，一旦数据包和某行匹配，执行该行规则，不再进行后续比较。

(3) 最后一行隐含“deny”的意义。如果数据包与访问列表中的所有行都不匹配，将被丢弃。

(4) IP 访问控制列表会发送一个 ICMP 主机不可达的消息到数据包的发送者，然后丢弃数据包。

(5) 如果某个列表挂接在实际接口上，删除列表后，默认的 deny any 规则会阻断那个接口的所有数据流量。

【试题 5】答　案：(58)B。

解　析：配置访问控制列表最关键的命令是 permit 和 deny。它们用来表示满足访问表项的报文是允许通过接口，还是要过滤掉。permit 表示允许报文通过接口，而 deny 表示匹配标准 IP 访问表源地址的报文要被丢弃。访问控制列表的条件语句是从第一句开始顺序执行的，只有与这个判断不相符合，才继续往下执行条件语句。

访问控制列表的配置工作的步骤主要包括：先定义一个标准、扩展或命名的访问控制列表，接着为该访问控制列表配置包过滤的准则，最后为这个访问控制列表配置应用接口。

【试题 6】答　案：(11)D；(12)B。

解　析：AUI 端口：就是用来与同轴电缆连接的接口，它是一种 D 型 15 针接口，是令牌环网或总线型网络中比较常见的端口之一。

RJ-45 端口：该端口是我们最常见的端口，即双绞线以太网端口。因为在快速以太网中也主要采用双绞线作为传输介质，所以根据端口的通信速率不同，RJ-45 端口又可分为 10Base-T 网 RJ-45 端口和 100Base-TX 网 RJ-45 端口两类。其中，10Base-T 网的 RJ-45 端口在路由器中通常标识为“ETH”，而 100Base-TX 网的 RJ-45 端口则通常标识为“10/100bTX”。

Console 接口：Console 端口使用配置专用连线直接连接至计算机的串口，利用终端仿真程序(如 Windows 系统下的“超级终端”)进行路由器本地配置。路由器的 Console 端口多为 RJ-45 端口。

Serial 接口：路由器的广域网连接中，应用最多的端口还要算“高速同步串口”(Serial)了，这种端口主要用于连接目前应用非常广泛的 DDN、帧中继(Frame Relay)、X.25、PSTN(模拟电话线路)等网络连接模式。

【试题 7】答　案：(28)B；(29)C。

解　析：静态路由是指由用户或网络管理员手工配置的路由信息。当网络的拓扑结构或链路的状态发生变化时，网络管理员需要手工去修改路由表中相关的静态路由信息。静态路由信息在缺省情况下是私有的，不会传递给其他路由器。当然，网管员也可以通过对路由器进行设置使之成为共享的。静态路由一般适用于比较简单的网络环境，在这样的环境中，网络管理员易于清楚地了解网络的拓扑结构，便于设置正确的路由信息。使用静态路由的另一个好处是网络安全保密性高。动态路由因为需要路由器之间频繁地交换各自的路由表，而对路由表的分析可以揭示网络的拓扑结构和网络地址等信息。因此，网络出于安全方面的考虑也可以采用静态路由。不占用网络带宽，因为静态路由不会产生更新流量。静态路由配置命令格式：ip route 目的网络 子网掩码 下一跳地址(或本地出口)。路由得查看路由表而决定怎么转发数据包，用静态路由一个个地配置，烦琐易错。如果路由器有个邻居知道怎么前往所有的目的地，可以把路由表匹配的任务交给它，省很多事。可以通过配置默认路由方式，其配置命令为：ip route 0.0.0.0 0.0.0.0 下一跳地址(或本地出口)。因特网所有的分组转发都是基于目的主机所在的网络，但在大多数情况下都允许有这样的特例，即对特定的目的主机指明一个路由。这种路由就叫作特定主机路由。

采用特定主机路由可使网络管理人员更方便地控制网络和测试网络，同时也可在需要考虑某种安全问题时采用这种特定主机路由。

主机路由格式：ip route 目的主机 IP 255.255.255.255 下一跳地址(或本地出口)。

9.4.4　案例分析试题参考答案

试题 1　答案与解析

答　案：

【问题 1】

(1) NAT；(2) ACL；(3) 静态 NAT；(4) 端口复用。

【问题 2】

(5) Deny；

(6) permit ip any 202.102.100.0 0.0.0.255；

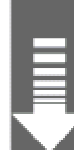
(7) 61.192.93.100 61.192.93.102；

(8) 202.102.100.100 202.102.100.102；

(9) list 101 pool ISP-B overload；

(10) 192.168.1.100 61.192.93.100 80；

(11) 192.168.1.100 202.102.100.100 80。



【问题 3】

(12) IP NAT OUTSIDE；

(13) IP NAT OUTSIDE；

(14) IP NAT INSIDE；

(15) IP ROUTE 61.192.93.0 255.255.255.0 S0；

(16) IP ROUTE 0.0.0.0 0.0.0.0 S1；

(17) 配置浮动默认路由。

【问题 4】

(18) 区分服务；

(19) 尽力而为服务；

(20) 尽力而为服务。

解　析：

【问题 1】

本题考查网络出口 NAT 的双线接入知识。

本问题主要考查 NAT 转换的相关知识。

一般来说，由于企业内网大都使用私有网络地址，私有地址只能在局域网中使用，不能出现在互联网上，那么使用私有地址的内部主机想要访问互联网，就必须使用地址转换技术将其转换为公有地址，也就是说如果内网用户想要访问互联网，就必须使用 NAT 地址转换技术，将私有地址转换为在互联网应用的公有地址。在使用 NAT 地址转换技术时，往往要使用 ACL 技术来指定允许转换的内部主机地址范围。

根据映射的方式，可以将 NAT 技术分为静态 NAT 和动态 NAT。其中，静态 NAT 是手工配置的内部私有地址和外部公共地址的对应关系，除非人工修改，否则不会变化，一般对外发布服务器使用静态 NAT 技术。动态 NAT 是多个内部主机和外部公共地址随机对应的一种方式，主要是通过指定内部允许转换的地址范围和外部允许使用的地址范围，然后对两个范围映射。这样具体外部的一个公共地址被内部哪台主机使用不确定。主要适用于企业内网大量用户的客户端访问外网。

【问题 2】

一个公司会与两个服务器供应商连接，这样做有利于提高内部访问 Internet 的速度和外网访问内部服务器的速度。由拓扑图可以看出该公司的出口路由器 Route-NAT 将 LAN 和 ISP-A 以及 ISP-B 连接，在 LAN 中有一台 Web 服务器需要发布到 Internet 上供外网访问。Route-NAT 上 S0 的接口地址是 61.192.93.100/24，可用于 NAT 的地址是 61.192.93.100～61.192.93.102，对端 ISP-A 的地址是 61.192.93.200/24。Route-NAT 上 S1 的接口地址是 202.102.100.100/24，可用于 NAT 的地址是 202.101.100.100～202.102.100.102，对端 ISP-B 的地址是 202.102.100.200。Route-NAT 内网口的地址是 192.168.1.1/24。

(1) 定义访问控制列表，由于需要根据访问的 IP 地址的不同来选择进行转换的 NAT 地址，所以需要使用扩展访问控制列表，控制 PAT 转换使用的地址池。

```
Route-Switch(config)#access-list 100 permit ip any 61.192.93.0 0.0.0.255
//定义到达 ISP-A 所有网段的 ACL
Route-Switch(config)#access-list 101 (deny) ip any 61.192.93.0 0.0.0.255
Route-Switch(config)#access-list 101 (permit ip any 202.102.100.0 0.0.0.255)
```

```
//定义到达 ISP-B 所有网段的 ACL
Access-list 100 定义了到达 ISP-A 的所有网段的 ACL，此处 61.192.93.0 代表 ISP-A 所有网段。
```

(2) 定义合法的地址池

```
Route-Switch(config)#ip nat pool ISP-A(61.192.93.101 61 192.93.102)netmask 255.255.255.0
//定义访问 ISP-A 的合法地址池
Route-Switch(config)#ip nat pool ISP-B(202.102.100.101 202.102.100.102)netmask 255.255.255.0
//定义访问 ISP-B 的合法地址池
```

(3) 配置 PAT 转换

```
Route-Switch(config)#ip nat inside source list100 pool ISP-A overload
Route-Switch(config)#ip nat inside source(list 101 pool ISP-B overload)
//为内网用户实现区分目标运营商网络进行匹配的 NAT 转换
```

(4) 配置静态 NAT，实现外网访问内网服务器

```
Route-Switch(config)#ip nat inside source static tcp (192.168.1.100 61.192.93.100)extendable
//为内网 Web 服务器配置 ISP-A 的静态 NAT 转换
Route-Switch(config)#ip nat inside source static tcp (192.168.1.100 202.102.100.100)extendable
//为内网 Web 服务器配置 ISP-B 的静态 NAT 转换
```

【问题 3】

通过路由选择原则，将 ISP-A 的目的地址配置静态路由并且下一跳指向 ISP 的路由器，再配置一条默认路由并且其下一跳指向 ISP-B 的路由器，最后再配置一条管理距离为 120 的默认路由，用以备份。

【问题 4】

QoS(Quality of Service，服务质量)指一个网络能够利用各种基础技术，为指定的网络通信提供更好的服务能力, 是网络的一种安全机制，是用来解决网络延迟和阻塞等问题的一种技术。在正常情况下，如果网络只用于特定的无时间限制的应用系统，并不需要 QoS，比如 Web 应用，或 E-mail 设置等，但是对关键应用和多媒体应用就十分必要。当网络过载或拥塞时，QoS 能确保重要业务量不受延迟或丢弃，同时保证网络的高效运行。通常 QoS 提供以下三种服务模型。

- Best-Effort service(尽力而为服务模型);
- Integrated service(综合服务模型，简称 Int-Serv);
- Differentiated service(区分服务模型，简称 Diff-Serv)。

试题 2 答案与解析

答 案：

【问题 1】

(1) Server；(2) 192.168.10.254；(3) 255.255.255.0；(4) range；(5) Trunk；(6) no switch port；(7) IP；(8) Routing；(9) Client；(10) trunk。





【问题 2】

(11) Permit；(12) list；(13) 192.168.40.1；(14) inside；(15) outside。

解　析：

【问题 1】

本题主要考查交换机的相关配置。

```
S1 (config)#vtp mode (server)//进入 vtp 服务器配置模式
S1 (config)#interface vlan 10
S1 (config-if)#ip address (192.168.10.254) (255.255.255.0)// VLAN10 采用 192.168.10.0/24 网段，每段最后一个地址作为网关地址
S1 (config)#interface (range) fastethernet 0/22-23 //进入 22 和 23 两个接口
S1 (config-if-range)#switchport mode (5) // 交换机默认为 access 模式，配置进入 trunk 模式
```

【问题 2】

本题考查交换机和路由器的基本配置。

根据题目的需求，使用交换机 S1 作为 VTP Server，规划整个网络的 VLAN 配置，同时使用三层交换机 S1 实现两个 VLAN 之间的通信，需在 S1 上创建 SVI 接口，并配置 IP 地址，关闭交换机的二层功能。

在 R1 上使用 NAT-PT 实现局域网的 Internet 访问，将连接内部局域网的接口设置内部接口并指定转换的外部接口 IP 地址，同时将连接 Internet 的接口设置为外部接口。

试题 3　答案与解析

答　案：

【问题 1】

(1)接口配置或端口配置；(2)192.168.1.1 255.255.255.0；(3)激活；(4)loopback 0；(5)192.168.1.20　255.255.255.255；(6)line vty0 4；(7)secret。

【问题 2】

(8)deny；(9)permit；(10)S0；(11)F0/0；(12)S0。

【问题 3】

(13)172.16.1.0 0.0.0.255 192.168.1.0 0.0.0.255；(14)enable；(15)202.102.100.1；(16)S0。

【问题 4】

(17)网络层；(18)隧道；(19)传输；(20)SA 或者安全关联。

解　析：

【问题 1】

```
RouterA>enable
RouterA#configure terminal
RouterA(config)#interface f0 / 0 // 进入 F0/0 的接口配置子模式
RouterA(config-if)#ip addr 192.168.1.1 255.255.255.0 // 为 F0/0 接口配置 IP 地址
RouterA(config-if)#no shut //激活 F0/0 接口，默认所有路由器的接口都为 down 状态
RouterA(config-if)#inter loopback 0 //进入 loopback 0 的接口配置子模式
```

RouterA(config-if)#ip addr 192.168.1.20 255.255.255.255 // 为 loopback 0 的接口配置 IP 地址
RouterA(config)#line vty 0 4 // 进入虚拟接口 0-4 的配置子模式
RouterA(config-line)#password abc001 //配置 vty 口令为“abc001”
RouterA(config)#enable password abc001 //配置全局配置模式的明文密码为“abc001”
RouterA(config)# enable secret abc001 //配置全局配置模式的密文密码为“abc001”

【问题 2】

RouterA(config)#access-list 101 deny ip 192.158.1.0 0.0.0.255 172.15.1.0 0.0.0.255
//拒绝来自 192.168.1.0/24 去往 172.16.1.0/24 网络的流量
RouterA(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 any
//定义需要被 NAT 的数据流
RouterA(config)#ip nat inside sourcelist 101 interface S0 overload
//NAT 转换关系(匹配 ACL101 的数据流都翻译成 S0 接口的公网 IP 地址，此为地址伪装)
RouterA(config)#int F0/0
RouterA(config-if)#ip nat inside //定义 NAT 的内部接口
RouterA(config)#int S0
RouterA(config-if)#ip nat outside //定义 NAT 的外部接口

【问题 3】

RouterB(config)#access-list 102 permit ip 172.15.1.0 0.0.0.255 192.168.1.0 0.0.0.255
//定义要通过 VPN 加密传输的数据流
RouterB(config)#crypto isakmp enable //启用 ISAKMP(IKE)
RouterB(config)#crypto isakmp policy 10 //建立 IKE 协商策略
RouterB(config-isakmp)#authentication pre-share //使用预定义密钥
RouterB(config-isakmp)#encryption des //加密算法
RouterB(config-isakmp)#hash md5 //HASH 算法
RouterB(config-isakmp)#group 2 //设置 1024 位 Diffie-Hellman 非对称加密算法
RouterB(config)#crypto isakmp identity address
//指定 ISAKMP 与分部路由器进行身份认证时使用 IP 地址作为标志
RouterB(config)#crypto isakmp key abc001 address 202.102.100.1 //指定共享密钥和对端设备地址
RouterB(config)#crypto ipsect ransform-set ccie esp-des esp-md5-hmac //配置 IPsec 交换集模式
RouterB(cfgcrypto-trans)#model tunnel //配置隧道模式
RouterB(config)#crypto map abc001 10 ipsec-isakmp //配置加密图
RouterB(config)#int S0
RouterB(config)-if)#crypto map abc001 //在外部接口上应用加密图

【问题 4】

本题考查 IPSec VPN 的基础知识。

IPSec (IP Security)是 IETF 为保证在 Internet 上传送数据的安全保密性而制定的框架协议，该协议应用在网络层，用于保证和认证用户 IP 数据包。IPSec 本身是开放的框架式协议，包含的各种算法之间是相互独立的，而且可以确保信息的机密性、数据的完整性、用



户的验证和防重发保护，所以在架设 VPN 时通常会使用 IPSec 协议来提供数据安全。

IPSecVPN 可使用的模式有两种，隧道模式和传输模式。使用隧道模式，IPSec 对整个 IP 数据包进行封装和加密，隐蔽了源和目的 IP 地址，从外部看不到数据包的路由过程，比较安全。而传输模式，IPSec 只对 IP 有效数据载荷进行封装和加密，IP 源和目的 IP 地址不加密传送，安全程度较低。

IPSec 主要由 AH、ESP 和 IKE 组成，在使用 IKE 协议时，需要定义 IKE 协商策略，该策略由 SA (安全关联)进行定义。配置 SA 是配置其他 IPSec 的前提，它定义了通信双方保护数据流的策略。

第 10 章

网 络 管 理

10.1 备考指南

10.1.1 考纲要求

根据考试大纲中相应的考核要求，在“网络管理”知识模块上，要求考生掌握以下方面的内容。

(1) 网络管理的功能域。

(2) 网络管理协议。

(3) 网络管理命令。

(4) 网络管理工具。

(5) 网络管理平台。

(6) 分布式网络管理。

10.1.2 考点统计

“网络管理”知识模块在历次网络工程师考试试卷中出现的考核知识点及分值分布情况如表 10.1 所示。

表 10.1 历年考点统计表

年 份	题 号	知 识 点	分 值
2017 年下半年	上午：46、47、59、63	SNMP 协议、RAID5 技术、arp-a 命令	4 分
	下午：无	无	0 分

续表

年　份	题　号	知 识 点	分　值
2017 年上半年	上午：46	网络管理命令	1 分
	下午：无	无	0 分
2016 年下半年	上午：47、48	SNMP 协议、arp 命令	2 分
	下午：无	无	0 分
2016 年上半年	上午：49、50、64	ping 命令、tracert 命令	3 分
	下午：无	无	0 分
2015 年下半年	上午：33、34、46、49、50	nslookup 命令、SNMP 协议、netstat 命令	5 分
	下午：无	无	0 分
2015 年上半年	上午：34、44～48、53	ipconfig 命令、SNMP 协议、故障管理、tracert 命令、netstat 命令、ping 命令	7 分
	下午：无	无	0 分
2014 年下半年	上午：28～30、33、50	Sniffer 报文分析、tracert 命令、netstat 命令、SNMPv2 操作	3 分
	下午：无	无	0 分
2014 年上半年	上午：34、35、47～49	网络流量计算、nslookup 命令、RMON、SNMPc、SNMP 支持的数据类型	4 分
	下午：无	无	0 分
2013 年下半年	上午：34、38、47～50	nslookup 命令、arp-a 命令、SNMPc 软件、MIB-2 的系统组、SNMPv2	12 分
	下午：无	无	0 分
2013 年上半年	上午：50	SNMP 协议	2 分
	下午：无	无	0 分
2012 年下半年	上午：46、47	SNMP 协议	4 分
	下午：无	无	0 分
2012 年上半年	上午：38、39、48、49	SNMPv2、arp-a 命令、嗅探器的工作原理	4 分
	下午：无	无	0 分

10.1.3　命题特点

纵观历年试卷，本章知识点是以选择题的形式出现在试卷中的。本章知识点在历次考试上午试卷中，所考查的题量为 5～6 道选择题，所占分值为 5～6 分(约占试卷总分值 75 分中的 8%～9%)。大多数试题是检验考生对相关理论知识点的理解，考试难度较低。

10.2 考点串讲

10.2.1 网管系统的功能及构成

网络管理就是通过某种方式对网络进行管理，使网络能正常高效地运行。其目的很明确，就是使网络中的资源得到更加有效的利用。它应维护网络的正常运行，当网络出现故障时能及时报告和处理，并协调、保持网络系统的高效运行等。

10.2.1.1 网络管理功能

在 OSI 系统管理标准中，将开放系统的管理功能划分为 5 个功能领域：配置管理、性能管理、故障管理、安全管理和计费管理功能领域。这 5 个功能领域覆盖了网络管理所需的主要功能，为网络管理系统的功能分析、设计和实现提供了基本保障。

1. 配置管理

配置管理是最基本的网络管理功能，负责监测和控制网络的配置状态。具体地讲，就是在网络建立、扩充、改造以及业务的开展过程中，对网络的拓扑结构、资源配备、使用状态等配置信息进行定义、监测和修改。

2. 性能管理

性能管理用来保证有效地运营网络并提供约定的服务质量，并在保证各种业务的服务质量(QoS)的同时，尽量提高网络资源的利用率。性能管理包括性能监测功能、性能分析功能和性能管理控制功能。

3. 故障管理

故障管理的作用是迅速发现和纠正网络故障，动态维护网络的有效性。故障管理的主要功能有报警监测、故障定位、测试、业务恢复以及修复等，同时还有维护故障日志的功能。

4. 安全管理

安全管理的作用是提供信息的保密、认证和完整性保护机制，使网络中的服务、数据和系统免受侵扰和破坏。安全管理主要包含风险分析功能，安全服务功能，告警、日志和报告功能以及网络管理系统保护功能。

5. 计费管理

计费管理的作用是正确地计算和收取用户使用网络服务的费用，进行网络资源利用率的统计和网络的成本效益核算。计费管理主要提供费率管理功能和账单管理功能。

10.2.1.2 网管系统的构成

一个完整的网络管理系统由多个部件组成，主要包括：网络管理协议、网络管理工作站、被管网络部件、管理信息库(MIB)。



作为管理者(Manager)，一个网络系统中可以有一个(或者几个)网络管理工作站；被管理者称作代理(Agent)，网上具有多个被管网络部件；网络管理协议是管理者和被管理者之间的操作规范，而具体的操作对象则是管理信息的集合——管理信息库(Management Information Base，MIB)。

网络管理系统的基本工作流程如下。

(1) 在被管理部件上预置代理。

(2) 网络管理者使用网络管理协议从代理的 MIB 中取得被管网络部件的管理信息，并存入自己的 MIB。

(3) 管理软件通过对 MIB 的分析处理，达到网络监控的管理目的。

10.2.2　网络管理协议

网络管理协议是管理者和被管理者之间共同遵循的规则，它们之间可以通过网络管理协议完成管理信息的交换任务。常用的网络管理协议包括 SNMP、MIB-Ⅱ和 RMON 等，它们都是基于 TCP/IP 协议工作的。

10.2.2.1　SNMP

1. SNMP 概述

SNMP 的前身是简单网关监控协议(SGMP)，用来对通信线路进行管理。随后对其改进并加入了符合 Internet 定义的 SMI 和 MIB 体系结构，改进后的协议就是著名的 SNMP。SNMP 的目标是管理 Internet 上众多厂家生产的软硬件平台，因此，SNMP 受 Internet 标准网络管理框架的影响很大。SNMP 的体系结构如图 10.1 所示。

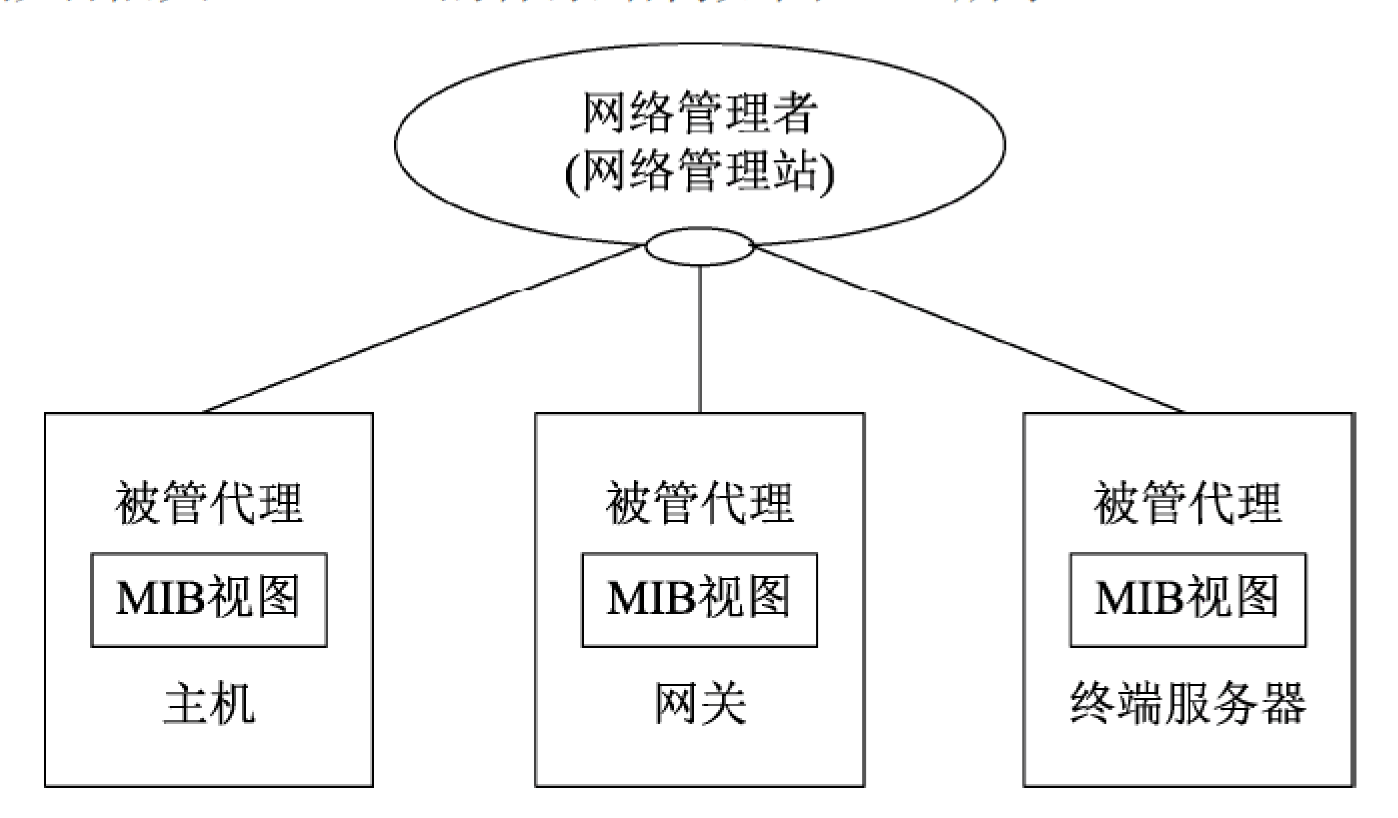


图 10.1　SNMP 的体系结构

SNMP 的体系结构围绕以下 4 个概念和目标进行设计。

- 使管理代理的软件成本尽可能低。
- 最大限度地保持远程管理的功能，以便充分利用 Internet 的网络资源。
- 体系结构必须有扩充的余地。
- 保持 SNMP 的独立性，不依赖于具体的计算机、网关和网络传输协议。

在 SNMP 改进版本 SNMPv2 中，又加入了保证 SNMP 体系本身安全性的目标。

另外，SNMP 中提供了以下 4 类管理操作。

- get 操作：用来提取特定的网络管理信息。
- get-next 操作：通过遍历操作来提供强大的管理信息的提取能力。
- set 操作：用来对管理信息进行控制(修改、设置)。
- trap 操作：用来报告重要的事件。

2. SNMP 管理控制框架与实现

1) SNMP 管理控制框架

SNMP 定义了管理进程(Manager)和管理代理(Agent)之间的关系，这个关系被称为共同体(Community)。描述共同体的语义是非常复杂的，但其句法很简单。位于网络管理工作站(运行管理进程)和各网络元素上，利用 SNMP 相互通信，并对网络进行管理的软件统称为 SNMP 应用实体。若干个应用实体和 SNMP 组合起来形成一个共同体。不同的共同体之间用名字来区分，共同体的名字必须符合 Internet 的层次结构命名规则，由非保留字符串组成。此外，一个 SNMP 应用实体可以加入多个共同体。

SNMP 的应用实体对 Internet 管理信息库中的管理对象进行操作。一个 SNMP 应用实体可操作的管理对象子集称为 SNMP MIB 授权范围。SNMP 应用实体对授权范围内管理对象的访问还有进一步的访问控制限制，比如只读、读/写等；SNMP 体系结构中要求每个共同体都规定其授权范围及其对每个对象的访问方式。记录这些定义的文件被称为共同体定义文件。

SNMP 的报文总是源自每个应用实体，报文中包括该应用实体所在的共同体的名字。这种报文在 SNMP 中称为有身份标识的报文，共同体名字是在管理进程和管理代理之间交换管理信息报文时使用的。管理信息报文中包括以下两部分内容。

- 共同体名：加上发送方的一些标识信息(附加信息)，用以验证发送方确实是共同体中的成员，共同体实际上就是用来实现管理应用实体之间身份鉴别的机制。
- 数据：这是两个管理应用实体之间真正需要交换的信息。

在第三版本前的 SNMP 中只是实现了简单的身份鉴别，接收方仅凭共同体名来判定收发双方是否在同一个共同体中，而前面提到的附加信息尚未应用。接收方在验明发送报文的管理代理或管理进程的身份后要对其访问权限进行检查。访问权限检查涉及以下因素。

- 一个共同体内各成员可以对哪些对象进行读、写等管理操作，这些可读写对象称为该共同体的授权对象(在授权范围内)。
- 共同体成员对授权范围内的每个对象定义了访问模式：只读或可读写。
- 规定授权范围内每个管理对象(类)可进行的操作(包括 get、get-next、set 和 trap)。
- 管理信息库(MIB)限制对每个对象的访问方式(如 MIB 中可以规定哪些对象只能读而不能写等)。

管理代理通过上述预先定义的访问模式和权限，来决定共同体中其他成员要求的管理对象访问(操作)是否允许。共同体概念同样适用于转换代理(Proxy Agent)，只不过转换代理中包含的对象主要是其他设备的内容。

2) SNMP 的实现方式

为了提供遍历管理信息库的手段，SNMP 在其 MIB 中采用了树状命名方法对每个管理对象的实例进行命名。每个对象实例的名字都是由对象类名字加上一个后缀构成，对象类

的名字是不会相互重复的，因而不同对象类的对象实例之间也很少有重名的危险。

在共同体的定义中一般要规定该共同体授权的管理对象的范围，相应地也就规定了哪些对象实例是该共同体的“管辖范围”，据此，共同体的定义可以想象为一个多叉树，以字典序提供了遍历所有管理对象实例的手段。有了这个手段，SNMP 就可以使用 get-next 操作符，顺序地从一个对象找到下一个对象。get-next(object-instance)操作返回的结果是一个对象实例的标识符及其相关信息，该对象实例在上面的多叉树中紧排在指定标识符 object-instance 对象的后面。这种手段的优点在于：即使不知道管理对象实例的具体名字，管理系统也能逐个地找到它，并提取到它的有关信息。遍历所有管理对象的过程可以从第一个对象实例开始(这个实例一定要给出)，然后逐次使用 get-next，直到返回一个差错(表示不存在的管理对象实例)结束(完成遍历)。

由于信息是以表格形式(一种数据结构)存放的，在 SNMP 的管理概念中，把所有表格都视为子树，其中一张表格(及其名字)是相应子树的根节点，每个列是根下面的子节点，一列中的每个行则是该列节点下面的子节点，并且是子树的叶节点，如图 10.2 所示。

因此，按照前面的子树遍历思路，对表格的遍历是先访问第一列的所有元素，再访问第二列的所有元素……直到最后一个元素。若试图得到最后一个元素的“下一个”元素，则返回差错标记。

SNMP 中各种管理信息大多以表格形式存在，一个表格对应一个对象类，每个元素对应于该类的一个对象实例。那么，管理信息表对象中单个元素(对象实例)的操作可以用前面提到的 get-next 方法，也可以用 get/set 等方法。下面主要介绍表格内一行信息的整体操作。

- 增加一行：通过 SNMP 只用一次 set 操作就可在一个表格中增加一行。操作中的每个变量都对应于待增加行中的一个列元素，包括对象实例的标识符。
- 删除一行：删除一行也可以通过 SNMP 调用 set 操作，将该行中的任意一个元素(对象实例)设置成“非法”即可。

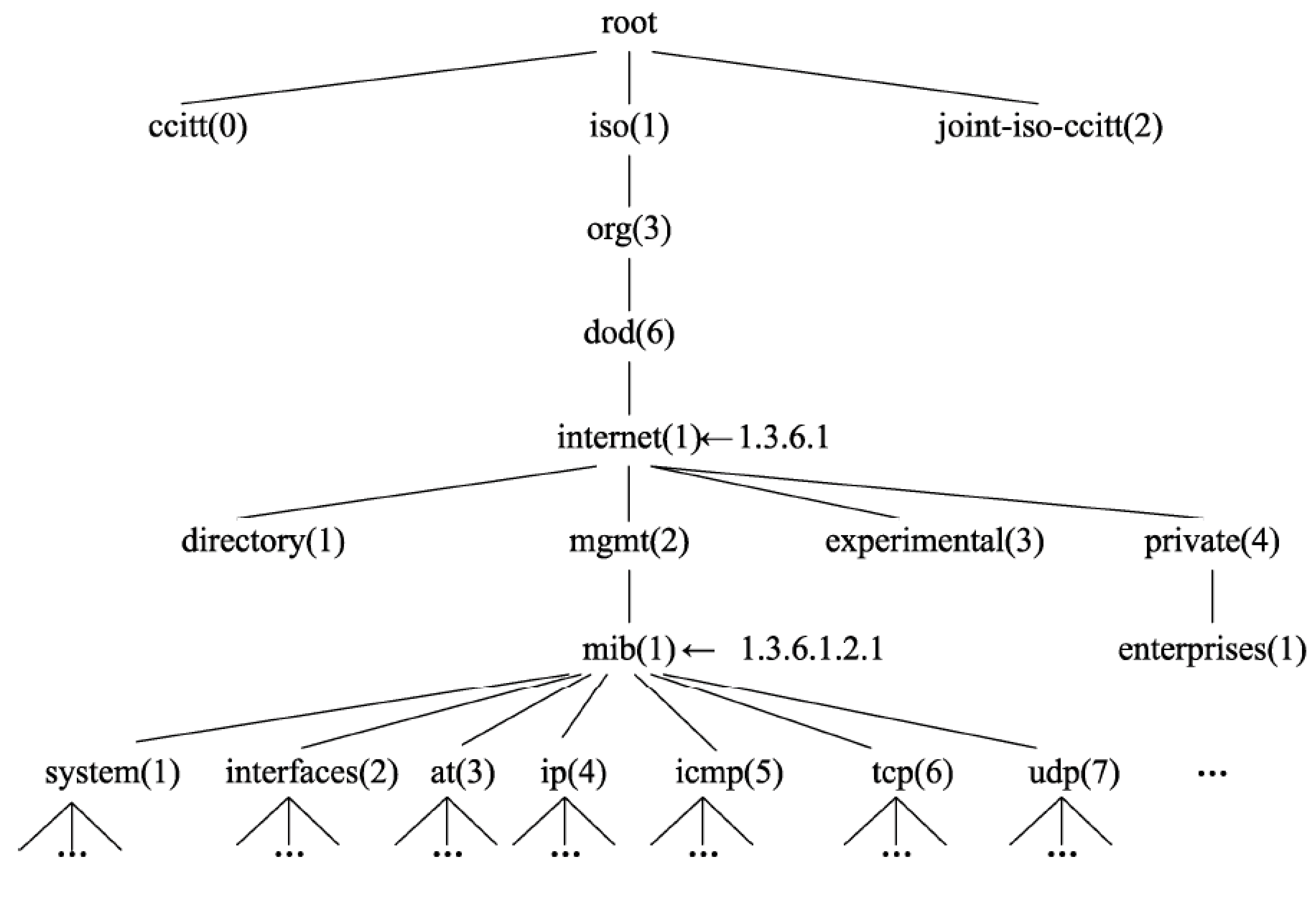


图 10.2　管理信息库中的对象标识

至于删除一行时，表中的一行元素是否真的在表中消失，则与每个设备(管理代理)的具体实现有关，因此管理进程必须能通过各数据字段的内容来判断数据的合法性。

3. SNMP 协议

SNMP 是一个异步的请求/响应协议，即 SNMP 的请求和响应之间没有必定的时间顺序关系，换句话说，SNMP 是一个面向无连接的协议。这样，SNMP 实体不需要在发出请求后立即等待响应的到来，因此 SNMP 响应也可能丢失或出现错误。

SNMP 协议是一个对称协议，没有主从关系，SNMP 上的管理进程和管理代理都可以得到 SNMP 完全相同的服务。下面对 SNMP 协议的部分特点和关键内容进行介绍。

1) 管理信息报文

在大多数 SNMP 操作中都使用一个相同的报文数据结构。对于前面提到的身份鉴别方法，报文中包含 3 种数据(信息)传递给专门的“身份鉴别实体”：共同体名称、有关数据和发送方 SNMP 实体的传输层地址。

身份鉴别实体负责验证发送方是否是合法的对等实体，并返回两种可能的结果：一种结果是返回本次报文中的 SNMP 协议数据类型和发送方 SNMP 实体的权限标识符；另一种结果是返回例外。其中第一种结果表明发送方 SNMP 实体确实是本共同体的成员之一，接收方 SNMP 实体接下来要对它进行处理；第二种结果(“例外”)表明发送方 SNMP 实体并非本共同体成员，不能接收此报文，并且接收方 SNMP 实体还可能根据配置产生一个“身份非法”的 trap 事件。

2) 协议数据单元及其管理操作

SNMP 协议实体之间的协议数据单元(PDU)有两种不同的结构和格式：一个 PDU 格式在大部分操作中使用，而另一个则只在 trap 操作中作为 trap 的协议数据单元。

PDU 一般包含多个代表特殊意义的字段：request-id 是一个整数值，用来区分不同的 PDU；error-status 反映管理操作是成功还是失败；error-index 表明操作中哪个变量错误；variable-bindings 是一系列变量的清单，序列中每一项包含一个变量名及其变量值。

在 SNMP 中，接收方完成身份鉴别并得到共同体定义信息之后，SNMP 实体便根据 PDU 内容执行几种操作：get 操作，根据变量名取出指定的对象实例；get-next 操作，该操作与 get 操作不同，不是取变量名指定的对象实例，而是按字典排序取出变量名指定的对象实例下一个对象实例；set 操作，对指定对象实体的值用请求中的新值替换；get-response 操作，对 get/set 报文做出响应并返回操作结果，收到该响应报文的操作请求方首先根据报文中的 request-id 在记录中查找有无这个序号的请求，如果没有则丢弃该响应，否则接收该响应，管理进程要进行响应处理。

3) trap 操作

trap 是一种捕捉事件并报告的操作，实际上几乎所有网络管理系统和管理协议都具有这种机制。trap 在 OSI 网络管理国际标准中称为“事件和通报”，一般都简称为事件报告。

为了减少管理信息的业务流量，管理代理负责对管理对象的 trap 进行检查，管理检查可以设置检查条件，这样，管理进程就可以在一定程度上控制 trap 报告过程。引入 trap 报告的最大好处是许多重要事件的发生得以及时让管理进程知道。因为一般只有比较关键的 trap 事件才确实需要报告，再加上每个 trap 事件都很简短，因此由于 trap 而引入的不确定管



理信息业务量是较少的，但能大大改善网络管理的时效性。

由于事件多种多样，各种事件发生环境也很不一样，因此 trap 操作的复杂性比前面讲的几种操作都大，SNMP 的 trap 操作 PDU 中的字段类型也较多。这些 trap 操作 PDU 中的字段包括：enterprise，记录发送 trap 事件的管理代理的标识符；agent-addr，管理代理的网络节点地址；generic-trap，描述该 trap 操作报告是哪一种异常事件；specific-trap，给出各管理代理自行定义的 trap 事件代码；time-stam，表示 trap 事件发生的时刻；variable-bindings，给出一组变量，这些变量及其值给出了与 trap 事件有关的详细信息。

当管理代理检测到一个例外或异常事件发生时，管理代理首先要判断需要将该事件报告给哪个或哪些管理进程。对每个管理进程，管理代理要选择相应的共同体号，由 SNMP 协议实体按照前面的字段格式构造 trap 报告的 PDU，再将其发送出去。

4)　SNMP PDU 的传输

SNMP 的设计是独立于具体的传输网络的，也就是说，它既可以在 TCP/IP 的支持下操作，也可以在 OSI 的传输层协议支持下完成操作，甚至可以在以太网的直接支持下实现操作。其中它对 OSI 传输层服务没有要求，既可以是有连接的服务，也可以是无连接的服务。为了实现上述目标，Internet 组织定义了若干个映射标准，规定了如何将 SNMP 协议数据单元 PDU 映射到下层的无连接传输请求上去。

在所有映射定义中，有一点是相同的，即所有 SNMP 报文数据是通过一个“顺序化”过程在网络上传输的，这个顺序化过程可以将任意结构的数据编码成一个有序的字符串进行传送。收到这些字符串，接收方按照完全相同的语法将它们解码成原来的数据结构。

5)　MIB 中为 SNMP 定义的管理对象

在 Internet 的第二版管理信息库 MIB-Ⅱ中，为 SNMP 应用实体定义了若干管理对象，其中包括 SNMP 的各种服务原语、各种收发协议数据单元、各种参数指示或统计变量等，凡 SNMP 中可操作的数据结构或变量都包括在内，下面将详细介绍。

10.2.2.2　MIB-II

在 TCP/IP 网络管理的建议标准中，提出了多个相互独立的 MIB，其中包含为 Internet 的网络管理而开发的 MIB-Ⅱ。鉴于它在说明标准 MIB 的结构、作用和定义方法等方面的重要性和代表性，有必要对其进行比较深入的探讨。

MIB-Ⅱ是在 MIB-Ⅰ的基础上开发的，是 MIB-Ⅰ的一个超集。MIB-Ⅱ组被分为以下分组。

- system：关于系统的总体信息。
- interfaces：系统到子网接口的信息。
- at(address translation)：描述 Internet 到子网的地址映射。
- ip：关于系统中 IP 的实现和运行信息。
- icmp：关于系统中 ICMP 的实现和运行信息。
- tcp：关于系统中 TCP 的实现和运行信息。
- udp：关于系统中 UDP 的实现和运行信息。
- egp：关于系统中 EGP 的实现和运行信息。
- dot3(transmission)：有关每个系统接口的传输模式和访问协议的信息。
- snmp：关于系统中 SNMP 的实现和运行信息。

1. system 组

system 组提供有关被管系统的总体信息。

2. interfaces 组

interfaces 组包含实体物理接口的一般信息，包括配置信息和各接口中所发生的事件的统计信息。

3. address translation 组

address translation 组由一个表构成，表中的每一行对应系统中的一个物理接口，提供网络地址向物理地址的映射。一般情况下，网络地址是指系统在该接口上的 IP 地址，而物理地址取决于实际采用的子网情况。例如，如果接口对应的是 LAN，则物理地址是接口的 MAC 地址；如果接口对应 X.25 分组交换网，则物理地址可能是一个 X.121 地址。

实际上，address translation 组包含在 MIB-Ⅱ中只是为了与 MIB-Ⅰ兼容，MIB-Ⅱ的地址转换信息在各个网络协议组中提供。

4. ip 组

ip 组包含有关节点上 IP 的实现和操作的信息，如有关 IP 层流量的一些计数器。ip 组中包含 3 个表：ipAddrTable、ipRouteTable 和 ipNetToMediaTable。

ipAddrTable 包含分配给该实体的 IP 地址的信息，每个地址被唯一地分配给一个物理地址。

ipRouteTable 包含用于互联网路由选择的信息，该路由表中的信息是从一些协议的路由表中抽取而来的。实体当前所知的每条路由都有一个条目，表格由 ipRouteDest 索引。ipRouteTable 中的信息可用于配置的监测，并且由于表中的对象是 read-write 的，因此也可被用于路由控制。

ipNetToMediaTable 是一个提供 IP 地址和物理地址之间对应关系的地址转换表，除了增加了一个指示映射类型的对象 ipNetToMediaType 之外，表中所包含的信息与 address translation 组相同。

此外，ip 组中还包含一些用于性能和故障监测的标量对象。

5. icmp 组

ICMP(Internet Control Message Protocol)是 TCP/IP 协议簇中的一部分，所有实现 IP 协议的系统都提供 ICMP。ICMP 提供从路由器或其他主机向主机传递消息的手段，它的基本作用是反馈通信环境中存在的问题。例如，数据报不能到达目的地，路由器没有缓冲区来转发数据报。

icmp 组包含有关一个节点的 ICMP 的实现和操作的信息，具体地讲，icmp 组是由节点接收和发送的各种 ICMP 消息的计数器所构成的一个表。

6. tcp 组

tcp 组包含有关一个节点的 TCP 的实现和操作的信息。

7. udp 组

udp 组包含有关一个节点的 UDP 的实现和操作的信息。除了有关发送和接收的数据包的信息之外，这个组中还包含一个 udpTable 表，该表中包含 UDP 端点的管理信息。所谓



UDP 端点是指正在支持本地应用接收数据报的 UDP 进程。udpTable 表中包含每个 UDP 端点用户的 IP 地址和 UDP 端口。

8. egp 组

egp 组包含有关一个节点的 EGP(External Gateway Protocol)的实现和操作的信息。除了有关发送和接收的 EGP 消息的信息之外，这个组中还包含一个 egpNeighTable 表，该表中包含有关相邻网关的信息。

10.2.2.3 RMON

简单网络管理协议(SNMP)是基于 TCP/IP 协议并在 Internet 中应用最广泛的网管协议，但是 SNMP 也有一些明显的不足，主要表现在以下 4 个方面。

- 由于 SNMP 使用轮询采集数据，而在大型网络中轮询会产生数量巨大的网络管理通信报文，导致网络交通拥挤甚至阻塞，故不适合管理大型网络。
- 不适合回收大信息量的数据，如一个完整的路由表。
- 基于 SNMP 的标准仅提供一般的验证，不能提供可靠的安全保证。
- 不支持 Manager-to-Manager 的分布式管理，它将收集数据的负担加在网管站上，使其成为瓶颈。

为了提高传送管理信息的可用性，减少管理站的负担，满足网络管理员监控网段性能的需求，IETF 开发了 RMON 以解决 SNMP 在日益扩大的分布式互连中的局限性。

远程网络监视(RMON)首先实现了对异构环境进行一致的远程管理，它为通过端口远程监视网段提供了解决方案。RMON 是 IETF 定义的 MIB(RFC 1757)，是对 SNMP 标准的扩展，它定义了标准功能以及在基于 SNMP 管理站和远程监控者之间的接口，主要实现对一个网段乃至整个网络的通信流量的监视功能，目前已成为网络管理标准之一。它可以对数据网进行防范管理，使 SNMP 更有效、更积极主动地监测远程设备，使网络管理员可以更快地跟踪网络、网段或设备出现的故障，然后采取防范措施，防止网络资源的失效。RMON MIB 的实现可以记录网络事件，即使在网络管理站没有与监控设备主动进行连接(脱机)的情况下也如此。另外，RMON MIB 也用于记录网络性能数据和故障历史，用户可以在任何时候访问故障历史数据以进行有效的故障诊断。使用这种方法减少了管理者同代理间的通信流量，使简单而有力地管理大型互联网络成为可能。

RMON 监视器可用两种方法收集数据：一种方法是通过专用的 RMON 探测仪，网管站直接从探测仪获取管理信息并控制网络资源，这种方法可以获取 RMON MIB 的全部信息；另一种方法是将 RMON 代理直接植入网络设备(路由器、交换机、Hub 等)，使其成为带 RMON Probe 功能的网络设施，网管站用 SNMP 的基本命令与其交换数据信息，收集网络管理信息，但这种方式受设备资源的限制，一般不能获取 RMON MIB 的所有数据，大多只收集 4 个组的信息。

RMON MIB 对网段数据的采集和控制通过控制表和数据表来完成。RMON MIB 按功能分成 9 个组，每个组都有自己的控制表和数据表(有些组两者合一，如统计组)。其中，控制表可以读写，数据表只能读，控制表用于描述数据表所存放数据的格式。配置的时候，由管理站设置数据收集的要求，存入控制表。开始工作后，RMON 监视器根据控制表的配置，把收集到的数据存放到数据表中。

RMON MIB 包含以下 9 组数据。

1) 统计组

统计组(Statistics)统计被监控的每个子网的基本统计信息。它能统计一个网段的流量(如交通流量的总包数和总字节数)，统计各种类型包的分布(如广播包、多点广播包、不同大小包的数量)，还能统计各种类型错误包数、碰撞次数等。

2) 历史组

历史组(History)定期地收集统计网络值的记录并为日后的处理把统计存储起来。它包含历史控制组和以太网历史组两个小组。其中历史控制组主要用来设置采样间隔时间等控制信息；以太网历史组为网络管理员提供有关网段流量、错误包、广播包、利用率以及碰撞次数等其他统计信息的历史数据。

3) 警报组

警报组(Alarm)允许网络管理站为网络性能(可以是监视器本地 MIB 的任意整数类型的对象)定义一组报警阈值，如果阈值在相应的方向上被越过，监视器就会产生警报并把警报发往网络管理站。

4) 主机组

主机组(Host)包含对连接在一个子网上所有主机的各种类型交通流量的记数值。它能够发现网上的新主机，对每个主机的 MAC 地址保持一组统计数据，例如，主机发送或接收的数据包总数、广播包数、流量字节数和错误包数等。它有一个控制表和两个数据表，且这两个数据表的内容相同，只是组织排列顺序不同。

5) 最高主机组

最高主机组(Host Top)包括排序后的主机统计，该报告基于主机表中的一些参数生成列表。它用于统计在一个子网上一些参数最高的一组主机，例如，它可以列出 10 个传输数据最多的主机，但依赖于主机组的实现。

6) 矩阵组

矩阵组(Matrix)用于记录关于子网上两个主机之间流量的信息，该信息以矩阵形式存储起来。这种方法对于检索特定主机之间的流量信息十分有用，例如，用于找出哪些设备对服务器的使用最多。矩阵组由 3 个表组成，即一个控制表加上两个数据表。

7) 过滤组

过滤组(Filter)允许监视器观测与过滤器相匹配的数据包。网络监视器可以捕获所有通过过滤器的数据包或简单地记下基于这些数据包的统计。

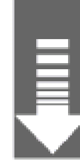
8) 包捕获组

包捕获组(Capture)控制数据被发往网管站的方式，它可以在把报文发送到某个通道后记录数据报文。

9) 事件组

事件组(Event)提供关于 RMON 代理所产生的所有事件的列表，当某事件发生时可以记录日志和发送 IRAP 到网管站。

尽管 RMON 有很多优点，但也有局限性：RMON 的 MAC 层探测器不能确定由服务器进入本地网段的数据包的源点和终点，或者是不能确定经过被监视网段的通信数据包的源点和终点。



1994 年，RMON2 工作组开始致力于提高现存的物理层和数据链路层之间的 RMON 规范，以实现在网络层和应用层提供历史和数据的统计服务。

在网络层，RMON2 通过监视点对点通信来记录网络使用的模式。另外，RMON2 还显示单个应用所占用的带宽，以及出现疑难故障的关键因素。

10.2.3　网络诊断和配置命令

10.2.3.1　ipconfig

ipconfig 工具用来显示所有当前的 TCP/IP 网络配置值、刷新动态主机配置协议(DHCP)和域名系统(DNS)设置。使用不带参数的 ipconfig 可以显示所有适配器的 IP 地址、子网掩码、默认网关。

1. 语法

ipconfig 的语法如下。

```
ipconfig [/all] [/renew [Adapter]] [/release [Adapter]] [/flushdns]
[/displaydns] [/registerdns] [/showclassid Adapter] [/setclassid Adapter
[ClassID]]
```

2. 参数

ipconfig 的参数如表 10.2 所示。

3. 注释

ipconfig 等价于 winipcfg，后者在 Windows Millennium Edition、Windows 98 和 Windows 95 上可用。

表 10.2　ipconfig 选项

选　项	描　述
/all	显示所有适配器的完整 TCP/IP 配置信息。在没有该参数的情况下，只显示 IP 地址、子网掩码和各个适配器的默认网关值
/renew [adapter]	更新所有适配器或特定适配器的 DHCP 配置。仅在具有配置为自动获取 IP 地址的网卡的计算机上可用
/release [adapter]	发送 DHCPRELEASE 消息到 DHCP 服务器，以释放所有适配器或特定适配器的当前 DHCP 配置并丢弃 IP 地址配置。同样仅在具有配置为自动获取 IP 地址的网卡的计算机上可用
/flushdns	清理并重设 DNS 客户解析器缓存的内容
/displaydns	显示 DNS 客户解析器缓存的内容，包括从本地主机文件预装载的记录以及由计算机解析的名称查询而最近获得的任何资源记录
/registerdns	初始化计算机上配置的 DNS 名称和 IP 地址的手工动态注册
/showclassid Adapter	显示指定适配器的 DHCP 类别 ID
/setclassid Adapter [ClassID]	配置特定适配器的 DHCP 类别 ID
/?	显示帮助信息

10.2.3.2 ping

ping 通过发送“Internet 控制报文协议(ICMP)”回送请求/应答报文来验证与另一台TCP/IP 计算机的 IP 级连接。回送请求/应答报文的接收情况将和往返过程的次数一起显示出来。ping 是用于检测网络连接性、可到达性和名称解析的疑难问题的主要 TCP/IP 命令，如果不带参数，ping 将显示帮助。

1. 语法

ping 的语法如下。

```
ping [-t] [-a] [-n Count] [-l Size] [-f] [-i TTL] [-v TOS] [-r Count] [-s
Count] [{-j HostList | -k HostList}] [-w Timeout] [TargetName]
```

2. 参数

ping 的参数如表 10.3 所示。

表 10.3　ping 选项

选　项	描　述
-t	中断前持续发送回送请求信息到目的地，按 Ctrl+Break 组合键中断并显示统计信息，按 Ctrl+C 组合键中断并退出
-a	对目的地 IP 地址进行反向名称解析，若解析成功，将显示相应的主机名
-n Count	指定发送回响请求消息的次数，默认值为 4
-l Size	指定发送消息中“数据”字段的长度，默认值为 32 B，最大值是 65 527 B
-f	指定发送的回响请求消息带有“不要拆分”标志，用于检测并解决“路径最大传输单位(PMTU)”的故障
-i TTL	指定发送回响请求消息的 IP 标题中的 TTL 字段值。其默认值是主机的默认 TTL 值。对于 Windows XP 主机，该值一般是 128。TTL 的最大值是 255
-v TOS	指定发送回响请求消息的 IP 标题中的“服务类型(TOS)”字段值。其默认值是 0。TOS 被指定为 0～255 的十进制数
-r Count	指定 IP 标题中的“记录路由”选项，用于记录由回响请求消息和相应的回响应答消息使用的路径。最小值必须为 1，最大值为 9
-s Count	指定 IP 标题中的“Internet 时间戳”选项，用于记录每个跃点的回响请求消息和相应的回响应答消息的到达时间。最小值为 1，最大值为 4
-j HostList	指定回响请求消息使用带有 HostList 指定的中间目的地集的 IP 标题中的“稀疏资源路由”选项。主机列表中的地址或名称的最大数为 9，用空格分开
-k HostList	指定回响请求消息使用带有 HostList 指定的中间目的地集的 IP 标题中的“严格来源路由”选项
-w Timeout	指定等待回响应答消息响应的时间(ms)，默认的超时时间为 4000 ms
TargetName	指定目的端，它既可以是 IP 地址，也可以是主机名

10.2.3.3 arp

arp 命令用于显示和修改 ARP 缓存中的项目。ARP 缓存中包含一个或多个表，它们用于存储 IP 地址及其经过解析的以太网或令牌环网物理地址。计算机上安装的每一个以太网或令牌环网络适配器都有自己单独的表。在没有参数的情况下使用，则 arp 命令将显示帮助



信息。

1. 语法

arp 的语法如下。

```
arp [-a [inet_addr] [-N if_addr]] [-g [inet_addr] [-N if_addr]] [-d
inet_addr [if_addr]] [-s inet_addr eth_addr [if_addr]]
```

2. 参数

arp 的参数说明如下。

- -a [inet_addr] [-N if_addr]：显示所有接口的当前 ARP 缓存表。要显示特定 IP 地址的 ARP 缓存项，请使用带有 inet_addr 参数的 arp -a 命令，此处的 inet_addr 代表 IP 地址。如果未指定 inet_addr，则使用第一个适用的接口。要显示特定接口的 ARP 缓存表，请将-N if_addr 参数与-a 参数一起使用，此处的 if_addr 代表指派给该接口的 IP 地址。-N 参数区分大小写。
- -g [inet_addr] [-N if_addr]：与-a 相同。
- -d inet_addr [if_addr]：删除指定的 IP 地址项，inet_addr 代表 IP 地址。对于指定的接口，要删除表中的某项，请使用 if_addr 参数。
- -s inet_addr eth_addr [if_addr]：向 ARP 缓存添加可将 IP 地址 inet_addr 解析成物理地址 eth_addr 的静态项。要向指定接口的表添加静态 ARP 缓存项，请使用 if_addr 参数。

10.2.3.4　netstat

netstat 工具可用来显示活动的 TCP 连接、计算机侦听的端口、以太网统计信息、IP 路由表、IPv4 统计信息(对于 IP、ICMP、TCP 和 UDP 协议)以及 IPv6 统计信息(对于 IPv6、ICMPv6、通过 IPv6 的 TCP 以及通过 IPv6 的 UDP 协议)。使用时如果不带参数，netstat 显示活动的 TCP 连接。

1. 语法

netstat 的语法如下。

```
netstat [-a] [-e] [-n] [-o] [-p Protocol] [-r] [-s] [Interval]
```

2. 参数

netstat 的参数介绍见表 10.4。

表 10.4　netstat 选项

选　项	描　述
-a	显示所有活动的 TCP 连接以及计算机侦听的 TCP 和 UDP 端口
-e	显示以太网统计信息，如发送和接收的字节数、数据包数。该参数可以与 -s 结合使用
-n	显示活动的 TCP 连接，不过，只以数字形式表现地址和端口号，却不尝试确定名称
-o	显示活动的 TCP 连接并包括每个连接的进程 ID(PID)，可以与 -a、-n 和 -p 结合使用
-p Protocol	显示 Protocol 所指定的协议的连接。在这种情况下，Protocol 可以是 TCP、UDP、TCPv6 或 UDPv6。如果该参数与-s 一起使用，按协议显示统计信息，则 Protocol 可以是 TCP、UDP、ICMP、IP、TCPv6、UDPv6、ICMPv6 或 IPv6

续表

选　项	描　述
-s	按协议显示统计信息。默认情况下，显示 TCP、UDP、ICMP 和 IP 协议的统计信息。若安装了 IPv6 协议，就会显示有关 IPv6 的 TCP、IPv6 上的 UDP、ICMPv6 和 IPv6 协议的统计信息。可以使用 -p 参数指定协议集
-r	显示 IP 路由表的内容。该参数与 route print 命令等价
Interval	每隔 Interval 秒重新显示一次选定的信息。按 Ctrl+C 组合键停止重新显示统计信息。如果省略该参数，netstat 将只打印一次选定的信息

10.2.3.5　tracert

tracert 通过递增，以“生存时间(TTL)”字段的值向目标发送“Internet 控制报文协议(ICMP)”回送请求/应答报文确定到达目标的路径。所显示的路径是源主机与目标主机间的路径中路由器的近侧路由器接口列表。近侧接口是距离路径中的发送主机最近的路由器的接口。不带参数时，tracert 显示帮助信息。

1. 语法

tracert 的语法如下。

```
tracert [-d] [-h MaximumHops] [-j HostList] [-w Timeout] [TargetName]
```

2. 参数

tracert 的参数说明如下。

- /d: 防止 tracert 试图将中间路由器的 IP 地址解析为它们的名称。
- -h MaximumHops: 在搜索目标(目的)的路径中指定跃点的最大数。其默认值为 30 个跃点。
- -j HostList: 指定“回响请求”消息对于在主机列表中指定的中间目标集使用 IP 报头中的“松散源路由”选项。可以由一个或多个具有松散源路由的路由器分隔连续的中间目的地。主机列表中的地址或名称的最大数为 9。主机列表是一系列由空格分开的 IP 地址(用带点的十进制符号表示)。
- -w Timeout: 指定等待“ICMP 已超时”或“回响答复”消息(对应于要接收的给定“回响请求”消息)的时间(以毫秒为单位)。如果超时时间内未收到消息，则显示一个星号(*)。默认的超时时间为 4000 ms(4s)。
- TargetName: 指定目标，可以是 IP 地址或主机名。

10.2.3.6　route

route 命令的功能是显示和修改本地的 IP 路由表，如果不带参数，则给出帮助信息。

1. 语法

route 的语法如下。

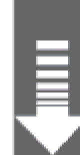
```
Route [-f] [-p] [Command [Destination] [mask Netmask] [Gateway] [metric
Metric] [if Interface]]
```

2. 参数

route 的参数说明如下。

- -f: 删除路由表中的网络路由、本地环路路由和组播路由。





- -p：与 add 命令联合使用时，一条路由被添加到注册表中，当 TCP/IP 协议启动时，用于初始化路由；与 print 命令联合使用时，则显示持久路由列表；对于其他命令，这个参数被忽略。
- Command：表示要运行的命令，可用的命令有 add(添加路由)、change(修改已有的路由)、delete(删除路由)和 print(打印路由)。
- Destination：说明目标地址，可以是网络地址、主机地址或默认路由。
- mask Netmask：说明目标地址对应的子网掩码。
- Gateway：说明下一跃点的 IP 地址。
- metric Metric：说明路由度量值，通常选择度量值最小的路由。
- if Interface：说明接口的索引。

10.2.3.7　pathping

pathping 是一个将 ping 和 tracert 的功能结合起来并有所增强的网络诊断工具，它可以反映出数据包从源主机到目标主机所经过的路径、网络延时以及丢包率，帮助用户解决网络问题。

1．语法

pathping 的语法如下。

```
pathping [-n] [-h maximum_hops] [-g host-list] [-p period] [-q num_queries]
[-w timeout] [-i address] [-R] [-T] [-4] [-6] target_name
```

2．参数

pathping 的参数介绍如下表 10.5 所示。

表 10.5　pathping 选项

选　项	描　述
-n	阻止 pathping 试图将中间路由器的 IP 地址解析为各自的名称
-h maximum_hops	指定搜索目标(目的)路径中存在的跃点的最大数。默认值为 30 个跃点
-g host-list	指定回响请求消息利用 host-list 中指定的中间目标集在 IP 数据头中使用“稀疏来源路由”选项。host-list 中的地址或名称的最大数为 9
-p period	指定两个连续的 ping 之间的时间间隔(以 ms 为单位)。默认值为 250 ms(1/4s)
-q num_queries	指定发送到路径中每个路由器的回响请求消息数。默认值为 100 个查询
-w timeout	指定等待每个应答的时间(以 ms 为单位)。默认值为 3000ms(3s)
-i address	指定源地址
-R	检查以确定路径中的每个路由器是否支持“资源保留协议”(RSVP)
-T	将 2 级优先级标记(例如，对于 IEEE 802.1p)连接到数据包并将它发送到路径中的每个网络设备上
-4	指定 pathping 只使用 IPv4
-6	指定 pathping 只使用 IPv6
target_name	指定目的端，它既可以是 IP 地址，也可以是主机名

10.2.3.8　nbtstat

nbtstat 命令是 Windows 自带的 NetBIOS 管理工具，用于显示本地计算机和远程计算机

基于 TCP/IP 协议的 NetBIOS 统计资料、本地计算机和远程计算机的 NetBIOS 名称表和 NetBIOS 名称缓存。nbtstat 可以刷新 NetBIOS 名称缓存和使用 Windows Internet 名称服务(WINS)注册的名称。使用不带参数的 nbtstat 则显示帮助信息。

1. 语法

nbtstat 的语法如下。

```
nbtstat [-a RemoteName] [-A IP address] [-c] [-n] [-r] [-R] [-RR] [-s] [-S]
[interval]
```

2. 参数

nbtstat 的参数介绍如表 10.6 所示。

表 10.6　nbtstat 选项

选　项	描　述
-a RemoteName	显示远程计算机的名称，并列出其名称列表。其中，RemoteName 是远程计算机的 NetBIOS 名称
-A IP address	显示远程计算机的 NetBIOS 名称表，其名称由远程计算机的 IP 地址指定。与-a 不同的是这个只能使用 IP，其实-a 就包括了-A 的功能
-c	显示远程计算机 NetBIOS 名称的缓存和每个名称的 IP 地址，此参数用来列出 NetBIOS 里缓存连接过的计算机的 IP
-n	显示本地计算机的 NetBIOS 名称表。Registered 的状态表明该名称是通过广播还是 WINS 服务器注册的
-r	显示 NetBIOS 名称解析统计资料。在配置为使用 WINS 且运行 Windows XP 或 Windows Server 2003 操作系统的计算机上，该参数将返回已通过广播、WINS 解析和注册的名称号码
-R	清除 NetBIOS 名称缓存的内容并从 Lmhosts 文件中重新加载带有#PRE 标记的项目
-RR	释放并刷新通过 WINS 服务器注册的本地计算机的 NetBIOS 名称
-s	显示 NetBIOS 客户端和服务器会话，并将目标 IP 地址转化为名称
-S	显示 NetBIOS 客户端和服务器会话，只通过 IP 地址列出远程计算机
interval	每隔“interval”秒重新显示选择的统计资料，按 Ctrl+C 组合键停止重新显示统计信息。如果省略该参数，nbtstat 将只显示一次当前的配置信息

注：NetBIOS 名称表是与运行在该计算机上的应用程序相对应的 NetBIOS 名称列表。

10.2.3.9　netsh

netsh 是一个命令行脚本实用程序，可用于修改计算机的网络配置。

利用 netsh 也可以建立批文件来运行一组命令，或者把当前的配置脚本用文本文件保存起来，以后可用来配置其他服务器。

1. netsh 上下文

netsh 利用动态链接库与操作系统的其他组件交互作用。netsh 助手是一个动态链接库文件，提供了称为上下文的扩展特性，可以对多种服务、实用程序或协议提供配置和监视功能。从一个上下文可以转到另一个上下文，后者叫作子上下文。



2. 在 Cmd.exe 命令提示符下运行 netsh 命令

为了在远程 Windows Server 2003 中运行 netsh 命令，首先要通过“远程桌面连接”连接到正在运行终端服务器的 Windows Server 2003 系统中。在 Cmd.exe 命令提示符下输入 netsh，就进入了 netsh>提示符。netsh 的语法如下。

```
netsh [-a AliasFile] [-c Context] [-r RemoteComputer] [{NetshCommand |-f
ScriptFile}]
```

- -a AliasFile：运行 AliasFile 文件后返回 netsh 提示符。
- -c Context：转到特定的 netsh 上下文。
- -r RemoteComputer：配置远程计算机。
- NetshCommand：说明要使用的 netsh 命令。
- -f ScriptFile：运行脚本后转出 netsh.exe。

10.2.3.10　nslookup

nslookup 是一个监测网络中 DNS 服务器是否能正确实现域名解析的命令工具。它通常需要一台域名服务器来提供域名服务。如果用户已经设置好域名服务器，就可以用这个命令查看不同主机的 IP 地址对应的域名。

1. 语法

nslookup 的语法如下。

```
nslookup [-SubCommand...] [{ComputerToFind | -Server}]
```

2. 参数

nslookup 的参数说明如下。

- -SubCommand…：将一个或多个 nslookup 子命令指定为命令行选项。
- ComputerToFind：如果未指定其他服务器，就使用当前默认 DNS 名称服务器查阅 ComputerToFind 的信息。要查找不在当前 DNS 域的计算机，请在名称上附加句点。
- -Server：指定将该服务器作为 DNS 名称服务器使用。如果省略了-Server，将使用默认的 DNS 名称服务器。

3. nslookup 的两种模式

nslookup 有两种模式：交互式和非交互式。

如果仅需要查找一块数据，应使用非交互式模式。对于第一个参数，输入要查找的计算机的名称或 IP 地址。对于第二个参数，输入 DNS 名称服务器的名称或 IP 地址。如果省略第二个参数，nslookup 使用默认 DNS 名称服务器。

如果需要查找多块数据，可以使用交互式模式。第一个参数输入连字符“(-)”，第二个参数输入 DNS 名称服务器的名称或 IP 地址；或者，省略两个参数，则 nslookup 使用默认 DNS 名称服务器。在交互方式下，可以用 set 命令设置选项，以满足指定的查询需要。下面是一些常用的子命令。

- >set all：列出当前设置的默认选项。
- set type=mx：查询本地域的邮件交换器信息。

- server NAME：由当前默认服务器切换到指定的名字服务器 NAME。
- ls：用于区域传输，罗列出本地区域中的所有主机信息。
- set type：设置查询的资源记录类型。DNS 服务器主要的资源记录有 A(域名到 IP 地址的映射)、PTR(IP 地址到域名的映射)、MX(邮件服务器及其优先级)、CNAM(别名)和 NS(区域的授权服务器)等类型。
- set type=any：对查询的域名显示各种可用的信息资源记录(A、CNAME、MX、NS、PTR、SOA 和 SRV 等)。
- set debug：显示查询过程的详细信息，这些信息可用于对 DNS 服务器进行排错。

10.2.3.11 net

在网络管理中，最常用的就是 net 命令家族。常用的 net 命令有以下几个。

- net view：用于显示正由指定的计算机共享的域、计算机或资源的列表。
- net share：用于管理共享资源，使网络用户可以使用某一服务器上的资源。
- net use：用于将计算机与共享的资源相连接或断开，或者显示关于计算机连接的信息。
- net start：用于启动服务，或显示已启动服务的列表。
- net stop：用于停止正在运行的服务。
- net user：可用来添加或修改计算机上的用户账户，或者显示用户账户的信息。
- net config：显示正在运行的可配置服务，或显示和更改服务器服务或工作站服务的设置。
- net send：用于将消息(可以是中文)发送到网络上的其他用户、计算机或者消息名称上。
- net localgroup：用于添加、显示或修改本地组。
- net accounts：可用来更新用户账户数据库、更改密码及所有账户的登录要求。

10.2.4 网络监视和管理工具

10.2.4.1 网络监听原理

在以太网中是基于广播方式传送数据的，也就是说，所有的物理信号都要经过其中的机器。如果将网卡置于混杂模式(Promiscuous)，那么网卡就能够接收到一切通过它的数据，而不管实际上数据的目的地址是不是它。

对于网卡来说一般有以下 4 种接收模式。

(1) 广播模式：在这种模式下，网卡能够接收网络中的广播信息。

(2) 组播模式：在这种模式下，网卡能够接收组播数据。

(3) 直接模式：在这种模式下，只有目的网卡才能接收该数据。

(4) 混杂模式：在这种模式下的网卡能够接收一切通过它的数据，而不管该数据是否是传给它的。



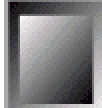
10.2.4.2　Sniffer

Sniffer，顾名思义就是侦听器、嗅探器或窃听器。其工作原理是：将网卡工作模式设置成混杂模式(Promiscuous Mode)，把所有发送到该网卡的数据全部接收下来，再对接收下来的数据进行分析。Sniffer 可以是软件，也可以是硬件，硬件的 Sniffer 常常被称作网络分析仪。最常见的 Sniffer 的软件产品有 Sniffer PRO/NetXray，它是一款专业的协议分析工具。

将 Sniffer 放置于被攻击机器或网络附近，可以很轻松地截获在网上传送的用户姓名、口令、信用卡号码、截止日期、账号和 PIN(个人识别码)。比如偷窥机密或敏感的信息数据，通过拦截数据包，入侵者可以很方便地记录别人之间敏感的信息传送，或者干脆拦截整个 E-mail 的会话过程。

10.2.4.3　网络管理平台

常见的网络管理软件有 HP 公司的 OpenView、IBM 公司的 NetView、Sun 公司的 SUN Net Manager、Cisco 公司的 Cisco Works 和 3Com 公司的 Transcend 等。



10.2.5　网络存储技术

10.2.5.1　廉价磁盘冗余阵列

廉价磁盘冗余阵列(Redundant Array of Inexpensive Disk，RAID)是利用一台磁盘阵列控制器管理一组磁盘驱动器，组成一个可靠的、快速的大容量磁盘系统。RAID 规范包括 RAID 0～RAID 7 等多个等级，目前投入到商业应用的有以下几种。

1. RAID 0

RAID 0 需要两个以上的磁盘驱动器，每个磁盘划分为不同的区块，数据按区块 A1、A2、A3…的顺序存储，数据访问采用交叉存取、并行传输的方式。这种系统具有最高的磁盘空间利用率，易管理，但系统的故障率高，属于非冗余系统。

2. RAID 1

RAID 1 由磁盘对组成，每一个工作盘都有其对应的镜像盘，上面保存着与工作盘完全相同的数据拷贝，具有最高的安全性，但磁盘空间利用率只有 50%。

3. RAID 2

RAID 2 采用了海明码纠错技术，用户需增加校验盘来提供单纠错和双验错功能。它对数据的访问涉及阵列中的每一个盘。大量数据传输时 I/O 性能较高，但不利于小批量数据传输，实际应用中很少使用。

4. RAID 3

RAID 3 把奇偶校验码存在一个独立的校验盘上，如果一个盘失效，其上的数据可以通过对其他盘上的数据进行异或运算得到；读数据很快，但因为写入数据时要计算校验位，速度较慢。RAID 3 主要用于图形图像处理等要求吞吐率比较高的场合，对于大量的连续数据可提供良好的传输速率，但对于随机数据，奇偶校验盘会成为写操作的瓶颈。

5. RAID 5

各块独立硬盘进行条带化分割，相同的条带区进行奇偶校验(异或运算)，校验数据平均分布在每块硬盘上。以 n 块硬盘构建的 RAID 5 阵列可以有 $n-1$ 块硬盘的容量，磁盘空间利用率为 $(n-1)/n$。它是目前使用得比较多的一种阵列。

6. RAID 0+1

RAID 0+1 是 RAID 0 和 RAID 1 的组合形式，也称为 RAID 10。RAID 0+1 是存储性能和数据安全兼顾的方案，它提供与 RAID 1 同样的数据安全保障的同时，也提供了与 RAID 0 近似的访问速率。

7. JBOD 模式

JBOD 代表 Just a Bunch of Drives，它是在逻辑上将几个物理磁盘连接起来，组成一个大的逻辑磁盘。JBOD 不提供容错，其容量等于所有磁盘容量的总和。从严格意义上说，JBOD 不属于 RAID 的范围。

10.2.5.2　网络存储

基于 Windows、Linux 和 UNIX 等操作系统的服务器称为开放系统，开放系统的数据存储方式如图 10.3 所示。

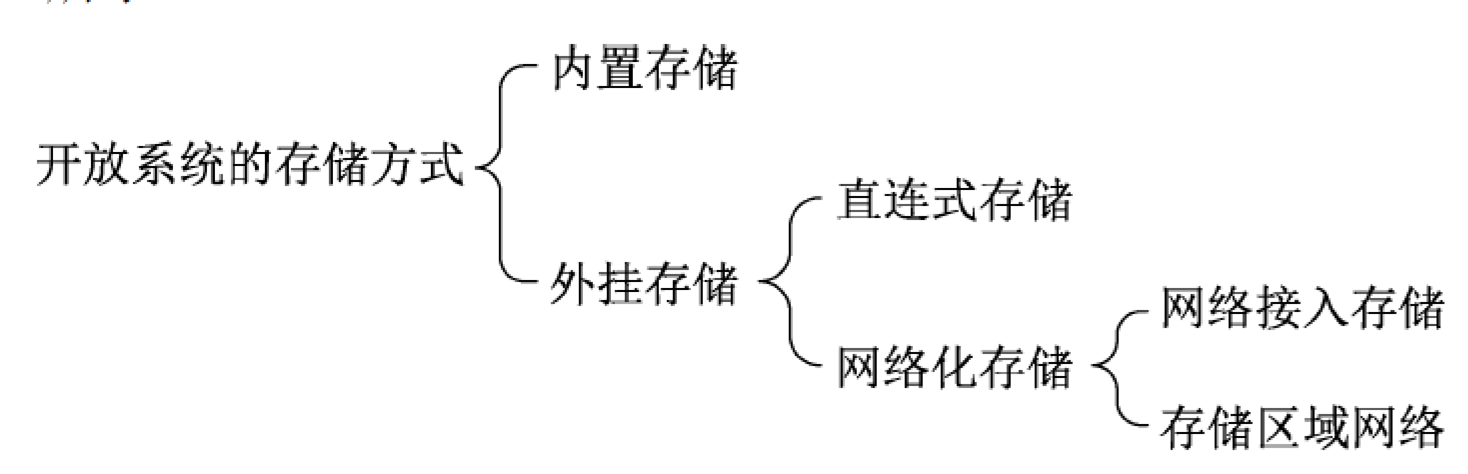


图 10.3　开放系统的数据存储方式

1. 直连式存储

直连式存储(Direct-Attached Storage，DAS)是在服务器上外挂一组大容量磁盘，存储设备与服务器主机之间采用 SCSI 通道连接，带宽为 10Mb/s、20Mb/s、40Mb/s 和 80Mb/s 等。这种方式难以扩展存储容量，而且不支持数据容错功能，当服务器出现异常时，会造成数据丢失。

2. 网络接入存储

网络接入存储(Network Attached Storage，NAS)是将存储设备连接到现有的网络上，来提供数据存储和文件访问服务的设备。NAS 服务器是在专用主机上安装简化了的瘦操作系统的文件服务器。NAS 服务器内置了与网络连接所需要的协议，可以直接联网，具有权限的用户可以通过网络来访问 NAS 服务器中的文件。

3. 存储区域网络

存储区域网络(Storage Area Network，SAN)是一种连接存储设备和存储管理子系统的专用网络，专门提供数据存储和管理功能。SAN 是一种特殊的高速网络，采用光纤通道实现互连，通过光纤通道交换机连接存储阵列和文件服务器主机。SAN 不仅能提供大容量的存



储数据，而且地域上可以分散部署，缓解了大量数据传输对局域网通信的影响。

10.3 真题详解

试题 1 (2017 年下半年试题 46)

在 SNMP 协议中，代理收到管理站的一个 GET 请求后，若不能提供该实例的值，则 (46) 。

(46) A. 返回下个实例的值　　B. 返回空值　　C. 不予响应　　D. 显示错误

参考答案：(46)A。

要点解析：正常情况下，返回管理站请求的每个值，如果不能够提供，没有相关值的时候，则返回下一个值。

试题 2 (2017 年下半年试题 47)

SNMP 是一种异步请求/响应协议，采用 (47) 协议进行封装。

(47) A. IP　　B. ICMP　　C.TCP　　D. UDP

参考答案：(47)D。

要点解析：SNMP 在传输层使用的是 UDP 协议。

试题 3 (2017 年下半年试题 59)

在 Windows 中，以下命令运行结果中不出现网关 IP 地址的是 (59) 。

(59) A. arp　　B. ipconfig　　C. netstat　　D. tracert

参考答案：(59)A。

要点解析：arp －a 虽然可以看到网关的 IP 和 MAC 地址，但不一定是网关地址。

试题 4 (2017 年下半年试题 63)

假如有 3 块容量是 300GB 的硬盘做 RAID5 阵列，则这个 RAID5 的容量是 (63) 。

(63)A. 300GB　　B. 4500B　　C. 600GB　　D. 900GB

参考答案：(63)C。

要点解析：RAID5 的容量占比为$(n-1)/n$，n 代表磁盘数量。

试题 5 (2017 年上半年试题 46)

某网络管理员在网络检测时，执行了 undo mac-address blackhole 命令。该命令的作用是 (46) 。

(46) A. 禁止用户接口透传 VLAN　　B. 关闭接口的 MAC 的学习功能
C. 为用户接口配置了端口安全　　D. 删除配置的黑洞 MAC

参考答案：(46)D。

要点解析：blackhole：目的黑洞 MAC 地址表项，当报文的目的 MAC 地址与目的黑洞 MAC 地址表项匹配后该报文被丢弃，undo mac-address blackhole 就是撤销 MAC 地址的黑洞。

试题6 (2016年下半年试题47)

SNMP 协议中网管代理使用__(47)__操作向管理站异步事件报告。

(47) A. trap　　B. set　　C. get　　D. get-next

参考答案：(47)A。

要点解析：SNMP 使用的是无连接的 UDP 协议，在运行代理程序的服务器端用 161 端口来接收 Get 或 Set 报文和发送响应报文(客户端使用临时端口)，但运行管理程序的客户端则使用熟悉的端口 162 来接收来自各代理的 Trap 报文。

试题7 (2016年下半年试题48)

从发现主机受到 ARP 攻击时需清除 ARP 缓存，使用的命令是__(48)__。

(48) A. arp -a　　B. arp -s　　C. arp -d　　D. arp -g

参考答案：(48)C。

要点解析：

arp -a：显示所有接口的 ARP 缓存表。

arp -s：添加一个静态的 ARP 表项。

arp -d：删除 ARP 缓存表项。

arp -g：与 arp -a 相同。

试题8 (2016年上半年试题49)

客户端采用 ping 命令检测网络连接故障时，可以 ping 通 127.0.0.1 及本机的 IP 地址，但无法 ping 通同一网段内其他工作正常的计算机的 IP 地址。该客户端的故障可能是__(49)__。

(49) A. TCP/IP 协议不能正常工作　　B. 本机网卡不能正常工作
C. 网络线路故障　　D. 本机 DNS 服务器地址设置错误

参考答案：(49)C。

要点解析：可以 ping 通 127.0.0.1 及本机的 IP 地址证明 TCP/IP、网卡均能正常工作；无法 ping 通同一网段内其他工作正常的计算机的 IP 地址，该故障和本机 DNS 服务器地址设置无关，故推断为网络线路故障。

试题9 (2016年上半年试题50)

在 Windows 的 DOS 窗口中输入命令

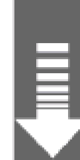
```
C:\>nslookup
>set type=ptr
>211. 151. 91. 165
```

这个命令序列的作用是__(50)__。

(50) A. 查询 211.151.91.165 的邮件服务器信息
B. 查询 211.151.91.165 到域名的映射
C. 查询 211.151.91.165 的资源记录类型
D. 显示 211.151.91.165 中各种可用的信息资源记录

参考答案：(50)B。

要点解析：PTR 记录也被称为指针记录，PTR 记录是 A 记录的逆向记录，作用是把 IP



地址解析为域名。

试题 10 （2016 年上半年试题 64）

使用 tracert 命令进行网络检测，结果如下所示，那么本地默认网关地址是__(64)__。

```
C:\>tracert 110.150.0.66
Tracing route to 110.150.0.66 over a maximum of 30 hops
1 2s 3s 2s 10.10.0.1
2 75ms 80ms 100ms 192.168.0.1
3 77ms 87ms 54ms 110.150.0.66
Trace complete
```

(64) A. 110.150.0.66　　B. 101.10.0.1
C. 192.168.0.1　　D. 127.0.0.1

参考答案：(64)B。

要点解析：tracert 是路由跟踪命令，用于确定 IP 数据包访问目标所采取的路径。根据题意，第一条就是本地网关返回的信息，那么本地默认网关就是 101.10.0.1。

试题 11 （2015 年下半年试题 33 和试题 34）

在 Windows 客户端运行 nslookup 命令，结果如图 10.4 所示。为 www.softwaretest.com 提供解析的是__(33)__。在 DNS 服务器中，ftp.softwaretest.com 记录通过__(34)__方式建立。

```
C:\Documents and Settings\user>nslookup www.softwaretest.com
Server:   nsl.softwaretest.com
Address: 192.168.1.254

Non-authoritative answer:
Name:    www.softwaretest.com
Address: 10.10.1.3

C:\Documents and Settings\user>nslookup ftp.softwaretest.com
Server:   nsl.softwaretest.com
Address: 192.168.1.254

Non-authoritative answer:
Name:    nsl.softwaretest.com
Address: 10.10.1.1
Aliases: ftp.softwaretest.com
```

图 10.4　命令运行结果

(33) A. 192.168.1.254　　B. 10.10.1.3
C. 10.10.1.1　　D. 192.168. 1.1

(34) A. 主机　　B. 别名　　C. 邮件交换器　　D. PIR 记录

参考答案：(33)A；(34)B。

要点解析：DNS 资源记录：

① SOA 记录：SOA 说明能解析这个区域的 DNS 服务器中哪个是主服务器。

② NS 记录：用于标识区域的 DNS 服务器，有几台提供服务。

③ A 记录：也称为主机记录，是 DNS 名称到 IP 地址的映射，用于正向解析。

④ PTR 记录：IP 地址到 DNS 名称的映射，用于反向解析。

⑤ MX 记录：邮件交换记录，在使用邮件服务器的时候，MX 记录是无可或缺的，比如 A 用户向 B 用户发送一封邮件，那么他需要向 DNS 查询 B 的 MX 记录，DNS 在定位到

了 B 用户的 MX 记录后反馈给 A 用户，然后 A 用户把邮件投递到 B 用户的 MX 记录邮件服务器里。

⑥ CNAME 记录：别名记录，这种记录允许将多个域名映射到同一台计算机。通常用于同时提供多种应用服务的计算机。例如，有一台计算机名为“host.csai.cn”(A 记录)。它同时提供 WWW 和 FTP 服务，为了便于用户访问服务，可以为该计算机设置两个别名(CNAME)：WWW 和 FTP。这两个别名的全称就是“www.csai.cn”和“ftp. csai.cn”。实际上它们都指向同一台计算机。

A 记录就是把一个域名解析到一个 IP 地址，而 CNAME 记录就是把域名解析到另外一个域名。其功能是差不多，CNAME 将几个主机名指向一个别名，其实跟指向 IP 地址是一样的，因为这个别名也要做一个 A 记录的。但是使用 CNAME 记录可以很方便地变更 IP 地址。如果一台服务器有 100 个网站，它们都做了别名，该台服务器变更 IP 地址时，只需要变更别名的 A 记录就可以了。

试题 12 (2015 年下半年试题 46)

根据图 10.5 所示的输出信息，可以确定的是 (46) 。

```
C:\>netstat-n

Active Connections

  Proto   Local Address          Foreign Address       State
  TCP     192.168.0.200:2011     202.100.112.12:443    ESTABLISHED
  TCP     192.168.0.200:2038     100.29.200.110:110    TIME_WAIT
  TCP     192.168.0.200:2052     128.105.129.30:80     ESTABLISHED
```

图 10.5 输出信息

(46) A. 本地主机正在使用的端口号是公共端口号
B. 192.168.0.200 正在与 128.105.129. 30 建立连接
C. 本地主机与 202.100.112.12 建立了安全连接
D. 本地主机正在与 100.29.200.110 建立连接

参考答案：(46)C。

要点解析：netstat -n 命令用于显示所有已建立的有效连接。连接状态如下。

① LISTEN：侦听来自远方的 TCP 端口的连接请求。
② SYN-SENT：在发送连接请求后等待匹配的连接请求。
③ SYN-RECEIVED：在收到和发送一个连接请求后等待对方对连接请求的确认。
④ ESTABLISHED：代表一个打开的连接。
⑤ FIN-WAIT-1：等待远程 TCP 连接中断请求，或先前的连接中断请求的确认。
⑥ FIN-WAIT-2：从远程 TCP 等待连接中断请求。
⑦ CLOSE-WAIT：等待从本地用户发来的连接中断请求。
⑧ CLOSING：等待远程 TCP 对连接中断的确认。
⑨ LAST-ACK：等待原来的发向远程 TCP 的连接中断请求的确认。
⑩ TIME-WAIT：等待足够的时间以确保远程 TCP 接收到连接中断请求的确认。
⑪ CLOSED：没有任何连接状态。



本机使用 3 个不同的端口号，通过 2011 端口与 202.100.112.12 建立了安全连接，通过 2052 端口与 128.105.129.30 建立了安全连接；通过 2038 端口正在与 100.29.200.110 进行连接中断。

试题 13　(2015 年下半年试题 49)

下列网络管理软件中不需要 SNMP 支持的是__(49)__。

(49) A. CiscoWorks　　B. Netview　　C. Solarwinds　　D. Wireshark

参考答案：(49)D。

要点解析：Wireshark(前称 Ethereal)是一个网络封包分析软件。网络封包分析软件的功能是撷取网络封包，并尽可能显示出最为详细的网络封包资料。Wireshark 使用 WinPCAP 作为接口，直接与网卡进行数据报文交换。

试题 14　(2015 年下半年试题 50)

在 SNMPv2 错误类型中，表示管理对象不可访问的是__(50)__。

(50) A. noAccess　　B. genErr

C. wrongValue　　D. noCreation

参考答案：(50)A。

要点解析：GetRequestPDU 的请求与 SNMPv2 相同，具有原子性。差别是处理相应的方式不同。分两个阶段处理这个请求：检验操作的合法性；更新变量。检验合法性包括：如果有一个变量不可访问，返回 noAccess；其他原因导致处理变量绑定对失败，用 genErr；指定值在任何情况下都不能赋予变量，用 wrongvalue；变量不存在，也不能生成，用 noCreation。

试题 15　(2015 年上半年试题 34)

查看 DNS 缓存记录的命令是__(34)__。

(34) A. ipconfig/flushdns　　B. nslookup

C. ipconfig/release　　D. ipconfig/displaydns

参考答案：(34)D。

要点解析：ipconfig/flushdns 用于刷新客户端 DNS 缓存的内容；ipconfig/release 用于向 DHCP 服务器发送 DHCP Release 请求，释放网卡的 DHCP 配置参数和当前使用的 IP 地址；ipconfig/displaydns 用于显示客户端 DNS 缓存的内容；nslookup 用于显示 DNS 查询信息，诊断和排除 DNS 故障。

试题 16　(2015 年上半年试题 44)

SNMP 协议属于__(44)__层协议。

(44) A. 物理　　B. 网络　　C. 传输　　D. 应用

参考答案：(44)D。

要点解析：本题考查 SNMP 方面的基础知识。

SNMP 为应用层协议，是 TCP/IP 协议簇的一部分。它通过用户数据报协议(UDP) 来操作。在分立的管理站中，管理者进程对位于管理站中心的 MIB 的访问进行控制，并提供网络管理员接口。管理者进程通过 SNMP 完成网络管理。

试题 17 (2015 年上半年试题 45)

SNMPv3 新增了__(45)__功能。

(45) A. 管理站之间通信　　B. 代理
C. 认证和加密　　D. 数据块检索

参考答案：(45)C。

要点解析：SNMPv3 主要增加 SNMP 在安全性和远端配置方面的功能。SNMPv3 提供的重要的安全性功能如下。

① 信息完整性：保证封包在传送中没有被篡改。
② 认证：检验信息来自正确的来源。
③ 封包加密：避免被未授权的来源窥探。

试题 18 (2015 年上半年试题 46)

网络管理系统中故障管理的目标是__(46)__。

(46) A. 自动排除故障　　B. 优化网络性能
C. 提升网络安全　　D. 自动监测故障

参考答案：(46)D。

要点解析：故障管理是网络管理中最基本的内容之一。故障管理的目的在于确保网络系统的高稳定性。在网络出现故障时，故障管理系统必须及时发现故障部位。故障管理的日常工作包含对所有节点动作状态的监控、故障记录的追踪与检查，以及平常对网络系统的测试。

试题 19 (2015 年上半年试题 47)

一台主机的浏览器无法访问域名为 www.sohu.com 的网站，并且在这台计算机执行 tracert 命令时有如下信息：

```
Tracing router to www.sohu.com [202.113.96.10] Over maximum of 30 hops:
1  <1ms  <1ms  <1ms  59.67.148.1
2  59.67.148.1  reports: Destination net unreachable
Trace complete
```

根据以上信息，造成这种现场的原因可能是__(47)__。

(47) A. 该计算机 IP 地址设置有误　　B. 相关路由器上进行了访问控制
C. 本地网关不可达　　D. 本地 DNS 服务器工作不正常

参考答案：(47)B。

要点解析：从命令执行结果中可看出 www.sohu.com 已经成功解析，可得出 IP 地址没问题，网关以及 DNS 正常工作。由提示 Destination net unreachable(无法到达目标网络)可知，问题应出在路由器上。

试题 20 (2015 年上半年试题 48)

使用 netstat -o 命令可显示网络__(48)__。

(48) A. IP、ICMP、TCP、UDP 协议的统计信息

B. 以太网统计信息

C. 以数字格式显示所有连接、地址及端口

D. 每个连接的进程 ID

参考答案：(48)D。

要点解析：netstat 命令是在内核中访问网络及相关信息的命令，能够显示协议统计和当前 TCP/IP 的网络连接。各参数含义如下。

-a：显示所有连接和监听端口。

-b：显示包含于创建每个连接或监听端口的可执行组件。

-e：显示以太网统计信息。此选项可以与-s 选项组合使用。

-n：以数字形式显示地址和端口号。

-o：显示与每个连接相关的所属进程 ID。

-p proto：显示 proto 指定的协议的连接。

-r：显示路由表。

-s：显示按协议统计信息。默认地，显示 IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP 和 UDPv6 的统计信息。

-v：与-b 选项一起使用时将显示包含于为所有可执行组件创建连接或监听端口的组件。

试题 21　(2015 年上半年试题 53)

如果要检查本机的 IP 协议是否工作正常，则应该 ping 的地址是＿(53)＿。

(53) A. 192.168.0.1　B. 10.1.1.1　C. 127.0.0.1　D. 128.0.1.1

参考答案：(53)C。

要点解析：127.0.0.1 是一个回送地址，指本地机，一般用 ping 127.0.0.1 来测试本地 TCP/IP 是否正常，如能 ping 通则说明正常。

10.4　强化训练

10.4.1　综合知识试题

试题 1　(2014 年下半年试题 28 和试题 29)

采用抓包工具截获的结果如图 10.6 所示，图中第 1 行记录显示的是＿(28)＿，该报文由＿(29)＿发出。

(28) A. TCP 错误连接响应报文　B. TCP 连接建立请求报文

C. TCP 连接建立响应报文　D. Urgent 紧急报文

(29) A. Web 客户端　B. Web 服务器　C. DNS 服务器　D. DNS 客户端

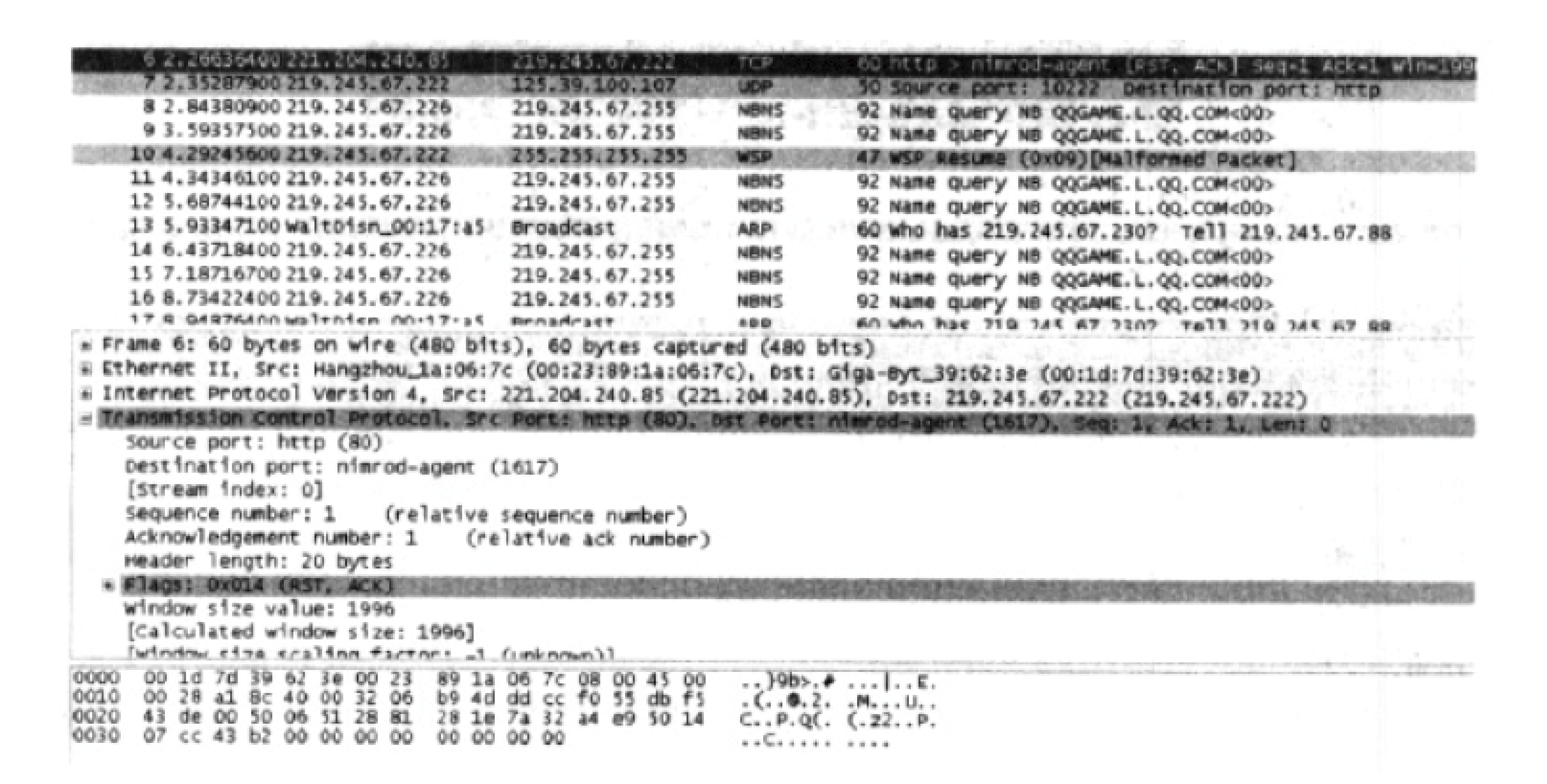


图 10.6　采用抓包工具截获的结果

试题 2　(2014 年下半年试题 30)

在 Windows 命令行窗口中输入 tracert 命令，得到图 10.7 所示窗口，则 PC 的 IP 地址可能为__(30)__。

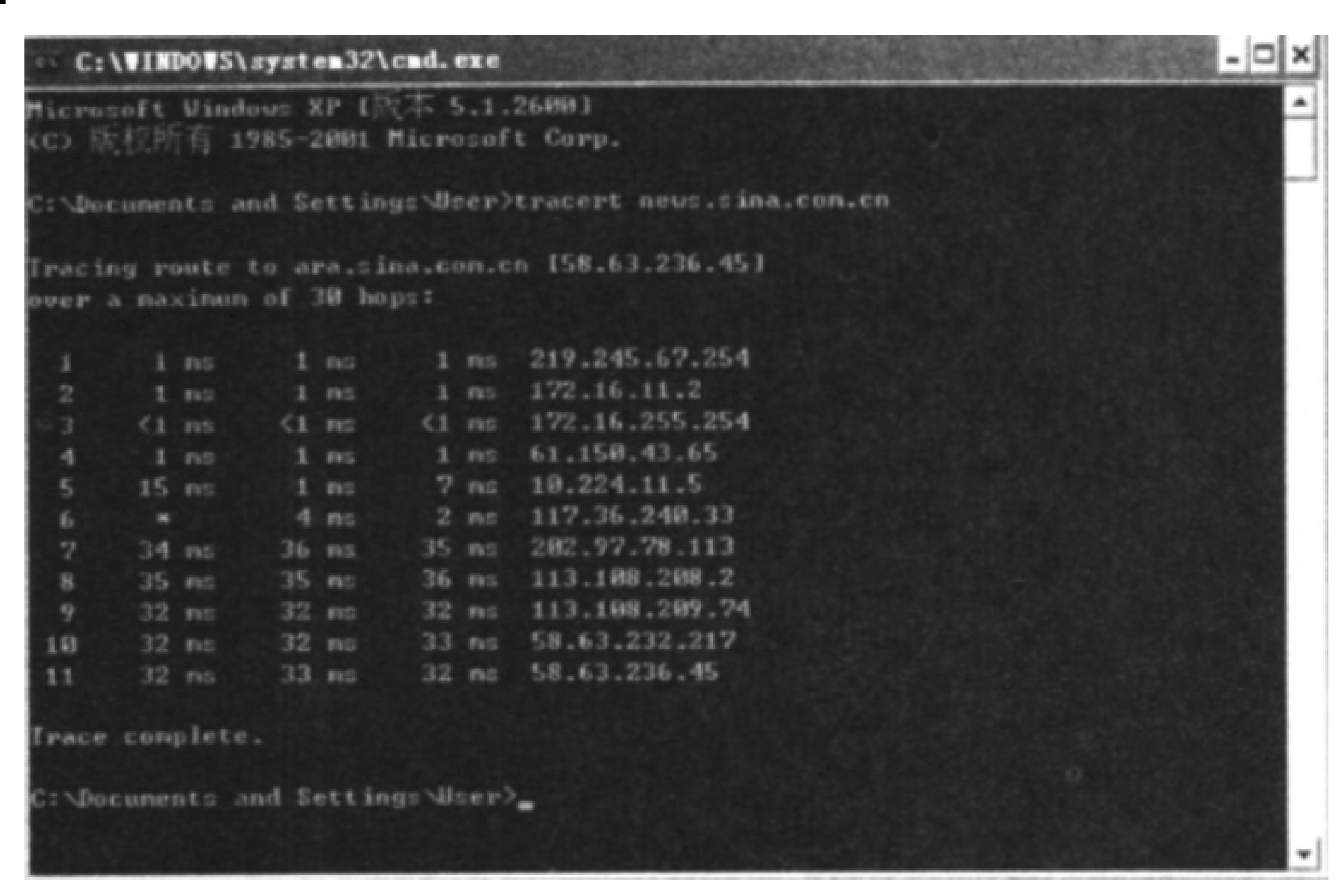


图 10.7　命令执行结果

(30) A. 172.16.11.13　　B. 113.108.208.1　　C. 219.245.67.5　　D. 58.63.236.45

试题 3　(2014 年下半年试题 33)

netstat -r 命令的功能是__(33)__。

(33) A. 显示路由记录　　B. 查看连通性
C. 追踪 DNS 服务器　　D. 捕获网络配置信息

试题 4　(2014 年下半年试题 50)

SNMPv2 的__(50)__操作为管理员提供了从被管设备中一次取回一大批数据的能力。

(50) A. GetNextRequest　　B. InformRequest
C. SetRequest　　D. GetBulkRequest



试题 5　(2014 年上半年试题 34)

假设网络的生产管理系统采用 B/S 工作方式，经常上网的用户数为 100 个，每个用户每分钟平均产生 11 个事务，平均事务量大小为 0.06MB，则这个系统需要的信息传输速率为__(34)__。

(34) A. 5.25Mb/s　　B. 8.8Mb/s　　C. 66Mb/s　　D. 528Mb/s

试题 6　(2010 年上半年试题 35)

在 Windows 命令行窗口中进入 nslookup 交互工作方式，然后输入 set type=mx，这样的设置可以__(35)__。

(35) A. 切换到指定的域名服务器　　B. 查询邮件服务器的地址
C. 由地址查找对应的域名　　D. 查询域名对应的各种资源

试题 7　(2014 年上半年试题 47)

管理站用 SetRequest 在 RMON 表中产生一个新行，如果新行的索引值与表中其他行的索引值不冲突，则代理产生一个新行，其状态对象的值为__(47)__。

(47) A. creatRequest　　B. underCreate　　C. valid　　D. invalid

试题 8　(2017 年上半年试题 48)

SNMPc 支持各种设备访问方式，在 SNMPc 支持的设备访问方式中，只是用于对 TCP 服务轮询的方式是__(48)__。

(48) A. 无访问模式　　B. ICMP(ping)　　C. SNMPv1 和 v2C　　D. SNMPv3

试题 9　(2014 年上半年试题 49)

下列数据类型中，SNMPv2 支持而 SNMPv1 不支持的是__(49)__。

(49) A. OCTET STRING　　B. OBJECT descriptor
C. Unsigned32　　D. Gauge32

10.4.2　综合知识试题参考答案

【试题 1】答　案：(28)A；(29)B。

解　析：本题考查 TCP 报头的标志位。第一行关键字 RST，是复位位，表示发生错误后发出的复位连接。通过详细报文可以看出源端口为 80，所以可以看出是 Web 端口发出去的。

【试题 2】答　案：(30)C。

解　析：第一次记录 219.245.67.254 响应时间最短，通常为本地局域网内其他机器的 IP，由此可以推断，本机的 IP 可能为 219.245.67.*。

【试题 3】答　案：(33)A。

解　析：netstat 命令用于显示各种网络相关信息，如网络连接、路由表、接口状态 (Interface Statistics)、masquerade 连接、多播成员 (Multicast Memberships)等。

常见参数：

-a (all)显示所有选项，默认不显示 LISTEN 相关。

-t (tcp)仅显示 tcp 相关选项。

-u (udp)仅显示 udp 相关选项。

-n 拒绝显示别名，能显示数字的全部转化成数字。

-l 仅列出正在 Listen (监听)的服务状态。

-p 显示建立相关链接的程序名。

-r 显示路由信息、路由表。

-e 显示扩展信息，例如 UID 等。

-s 按各个协议进行统计。

-c 每隔一个固定时间，执行该 netstat 命令。

【试题 4】答　案：(50)D。

解　析：简单网络管理协议(SNMP)，由一组网络管理的标准组成，包含一个应用层协议(Application Layer Protocol)、数据库模型(Database Schema)和一组资源对象。该协议能够支持网络管理系统，用以监测连接到网络上的设备是否有任何引起管理上关注的情况。

SNMP 的第一个版本是 SNMPv1，指定了五种核心 PDU：GET REQUEST、GET NEXT REQUEST、GET RESPONSE、SET REQUEST、TRAP。

SNMP 的第二个版本是 SNMPv2，增加了用于大量数据传输的 GetBulkRequest 和与管理站之间通信的 InformRequest。

【试题 5】答　案：(34)B。

解　析：用户数量 100 个，每个用户每分钟产生 11 个事务，意味着这 100 个用户每秒可以产生(100×11)/6 个事务，每个事务量大小为 0.06MB，亦即每个事务量的比特数为 0.06MB×8=0.48Mbits。系统计算的信息传输速率单位是 b/s，(100×11×0.48)/60=8.8Mb/s。

【试题 6】答　案：(35)B。

解　析：nslookup 命令中 set type=ResourceRecordType 指定 DNS 资源记录类型。默认的资源记录类型为 A。表 10.7 列出此命令的有效值。

表 10.7　命令有效值

值	说　明
A	指定计算机 IP 地址
ANY	指定所有数据类型
CNAME	指定用于别名的规范名称
GID	指定组名的组标识符
HINFO	指定计算机 CPU 以及操作系统类型
MB	指定邮箱域名
MG	指定邮件组成员
MINFO	指定邮箱或邮件列表信息
MR	指定邮件重命名域名
MX	指定邮件交换器
NS	指定用于命名区域的 DNS 名称服务器

续表

值	说　明
PTR	如果查询是 IP 地址，则指定计算机名；否则指定指向其他信息的指针
SOA	指定用于 DNS 区域的“起始授权机构”
TXT	指定文本信息
UID	指定用户标识符
UINFO	指定用户信息
WKS	描述已知服务

【试题 7】答　案：(47)A。

解　析：RMON(远程网监控协议)也是一种监控局域网通信的标准。它在 SNMP 管理信息库的基础上进行了扩充，能够实现离线操作、主动监视、问题检测和报告、提供增值数据、多管理站操作等。RMON 的目标是扩展 SNMP 的 MIB-2(管理信息库)使 SNMP 更为有效、更为积主动地监控远程设备。RMON MIBE 由一组统计数据、分析数据和诊断数据构成，利用许多供应商生产的标准工具都可以显示出这些数据，因而它具有独立于供应商的远程网络分析功能。

在 RMON 表操作管理中，管理站用 set 命令在 RMON 表中增加行，并遵循下列规则。

① 管理站使用 SetRequest 生成一个新行，如果新行的索引值不冲突，则代理产生一个新行，其状态值为 creatRequest。

② 新行产生后，由代理把状态对象值置为 underCreation。对于管理站没有设置新值的列对象，代理可以置为默认值，或者让新行维持这种不完整、不一致的状态。

③ 新行的状态保持为 underCreation，直到管理站产生了所要生成的新行。这时由管理站置每一新行状态的值为 valid。

④ 如果管理站要生成的新行已经存在，则返回一个错误值。

【试题 8】答　案：(48)A。

解　析：SNMPc 支持各种设备访问模式，包括 TCP、ICMP(ping)、SNMPv1、SNMPv2C 和 SNMPv3。

① 无访问模式(仅对 TCP)只用于对 TCP 服务的轮询，当 ICMP 或 SNMP 访问受防火墙限制时使用这种方式。

② ICMP(ping)方式用于不支持 SNMP，但是可以通过 ping 程序进行探测的设备。

③ SNMPv1 与 SNMPv2C 方式与当前大多数网络设备配置的 SNMP 代理协议相似。任何支持 SNMPv2C 的设备通常也支持 SNMPv1，两种模式之间自动切换，因此用户可以选择 SNMPv1 作为任何 SNMP 设备的访问模式。

④ SNMPv3 是安全的 SNMP 代理协议，支持身份验证和加密功能。

【试题 9】答　案：(49)C。

解　析：SNMPv1 支持的数据类型主要有。

INTEGER：整型，是-2^{31}～2^{31}之间的有符号整数。

OCTET STRING：字符串。

OBJECT IDENTIFIER：对象标识符。

IpAddress：以网络序表示的 32 位 IP 地址。

counter32：计数器是一个非负的整数，它递增至最大值，而后归零。SNMPv1 中定义的计数器是 32 位的。

Gauge32：也是一个非负整数，它可以递增或递减，但达到最大值时保持在最大值，最大值为 $2^{32}-1$。

TimeTicks：是一个时间单位，表示以 0.01 秒为单位计算的时间。

Opaque：表示用于传递任意信息串的任意编码格式，它与 SMI 使用的严格数据输入格式不同。

Unsigned32 的数据类型是 SNMPv1 所不支持的。

第 11 章 网络规划与设计

11.1 备考指南

11.1.1 考纲要求

根据考试大纲中相应的考核要求，在“网络规划与设计”知识模块上，要求考生掌握以下方面的内容。

(1) 网络系统的需求分析，包括功能需求、性能需求、可靠性需求、安全需求、管理需求。

(2) 网络系统的设计，包括拓扑结构设计、信息点分布和通信量计算、结构化布线、链路冗余和可靠性、安全措施、网络设备的选型。

(3) 通信子网的设计，包括核心交换机的选型和配置、汇聚层的功能配置、接入层交换机的配置和部署。

(4) 资源子网的设计，包括网络服务和服务器的选型。

(5) 网络系统的构建和测试，包括安装工作、测试和评估、转换到新网络的工作计划。

11.1.2 考点统计

“网络规划与设计”知识模块在历年网络工程师考试试卷中出现的考核知识点及分值分布情况如表 11.1 所示。

表 11.1 历年考点统计表

年 份	题 号	知 识 点	分 值
2017 年下半年	上午：65	层次化网络设计	1 分
	下午：试题二	企业网安全管理与配置	20 分

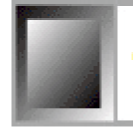
续表

年份	题号	知识点	分值
2017年上半年	上午：47～50、67～70	网络故障诊断、结构化布线系统、网络结构设计	8分
	下午：试题一	企业网的规划与设计	20分
2016年下半年	上午：29、68～70	结构化布线系统、逻辑网络设计	4分
	下午：试题二	企业网的规划与设计	20分
2016年上半年	上午：68～70	逻辑网络设计	3分
	下午：无	无	0分
2015年下半年	上午：48、68～70	网络故障诊断、层次化局域网模型	4分
	下午：试题一	企业园区网的规划与设计	20分
2015年上半年	上午：25、54、55、66、68、69	网络故障诊断、网络安全需求	6分
	下午：试题一	企业网的规划与设计	20分
2014年下半年	上午：34、67～70	结构化布线系统、逻辑网络设计、网络汇聚层	3分
	下午：试题一	企业网的规划与设计	15分
2014年上半年	上午：33、50、70	干线子系统、网络故障、物理网络设计	4分
	下午：试题一	园区网的部署	15分
2013年下半年	上午：无	无	0分
	下午：无	无	0分
2013年上半年	上午：70	网络系统设计	2分
	下午：试题一	校园网的规划与设计	15分
2012年下半年	上午：无	无	0分
	下午：试题一	校园网的规划与设计	20分
2012年上半年	上午：无	无	0分
	下午：试题一	企业网的规划与设计	15分

11.1.3 命题特点

纵观历年试卷，本章知识点是以选择题和综合分析题的形式出现在试卷中的。本章知识点在历次考试上午试卷中，所考查的题量大约为3～6道选择题，所占分值为3～6分(约占试卷总分值75分中的4%～8%)；在下午试卷中，所考查的题量大约为1道综合分析题，所占分值大约为15分(约占试卷总分值75分中的20%)。本章考题主要检验考生是否理解相关的理论知识点和实践经验，考试难度较高。从知识点考查深度的角度分析，每次考试这部分试题在“识记、理解、应用”3个层面上所占的比例大致为1∶1∶3。

11.2　考点串讲

 11.2.1　结构化布线系统

11.2.1.1　结构化布线系统的概念

结构化综合布线系统是基于现代计算机技术的通信物理平台，集成了语音、数据、图像和视频的传输功能，消除了原有通信线路在传输介质上的差别。

结构化综合布线系统包括：建筑物综合布线系统(Premises Distribution System，PDS)、智能大厦布线系统(Intelligent Building System，IBS)、工业布线系统(Industry Distribution System，IDS)。

建筑物综合布线系统(PDS)是一个能够支持任何用户选择的语音、数据、图形、图像应用的电信布线系统，系统应能支持语音、图形、图像、数据多媒体、安全监控、传感等各种信息的传输，支持 UTP、光纤、STP、同轴电缆等各种传输载体，支持多用户多类型产品的应用，支持高速网络的应用。

结构化综合布线系统应满足标准化、实用性、先进性、开放性、结构化和层次化的要求。

11.2.1.2　结构化布线系统的组成

结构化布线系统分为 6 个子系统：工作区子系统、水平子系统、管理子系统、干线子系统、设备间子系统和建筑群子系统。

1. 工作区子系统

工作区子系统是由终端设备到信息插座的整个区域，用于将用户终端设备连接到布线系统，主要包括信息插座、跳线、适配器。

信息插座的安装分为嵌入式和表面安装两种方式，信息插座通常安装在工作间四周的墙壁下方，距地面 30cm，也有的安装在用户办公桌上。通常一个信息插座需要 9 m^2 的空间。

2. 水平子系统

水平子系统是结构化综合布线系统中连接用户工作区与布线系统主干的子系统，由每层配线间至信息插座的配线电缆和工作区用的信息插座等组成。在结构化综合布线系统中，水平子系统起着支线的作用，它将所有用户端通过一些连接件连接到配线设备上。

水平布线的布线通道有两种：一种是暗管预埋、墙面引线方式；另一种是地下管槽、地面引线的方式。

3. 管理子系统

管理子系统是结构化布线系统中对布线电缆进行端接及配线管理的子系统，通常设置在楼层的接线间内。

管理子系统由各种交连设备(双绞线跳线架、光纤跳线架)以及集线器和交换机等交换设

备组成。交连设备通过水平子系统连接到各个工作区的信息插座上，集线器或交换机与交连设备之间通过短线缆互连，这些短线被称为跳线。

4. 干线子系统

干线子系统是结构化综合布线系统中连接各管理间、设备间的子系统，又称垂直子系统。综合布线系统的干线可根据距离的远近和用户对传输速率及传输质量的要求，选择多对数双绞线或光缆。一般在楼内的语音通信采用三类的大对数双绞线作为主干；数据通信可以采用高品质的五类双绞线，也可以采用光缆；如果电磁干扰严重，则推荐采用光缆作为数据主干。在做干线子系统的设计时，首先要确定每一层楼的干线需求，总结出整座楼的干线总体需求，确定干线电缆的种类及其大小尺寸，然后确定干线电缆的路由通道。

5. 设备间子系统

设备间子系统主要用来安放网络关键设备，地位十分重要。并非每一个综合布线系统都有设备间子系统，但在大型建筑物中一般是有的，而且有时还不止一个。设备间子系统中的电话、数据、计算机主机设备及其保安配线设备宜设在一个房内。必要时，也可以分别设置，但程控交换机及计算机主机房距离设备间不宜太远。设备间的位置及大小应根据设备的数量、规模、最佳网络中心等内容综合考虑确定。在设备间子系统的设计和安装过程中还需要综合考虑配电系统(不间断电源 UPS)和安全因素(设备接地等)。

6. 建筑群子系统

建筑群子系统是结构化综合布线系统中由连接楼群之间的通信传输介质及各种支持设备组成的子系统。建筑群子系统也称为户外子系统，其传输介质除了各种有线手段之外，还可包含其他无线通信手段，如微波、无线电通信等。

户外电缆在进入大楼时通常在入口处经过一次转接接入户内系统，在转接处可以加上电气保护设备。现代化电话通信系统中通信线路在进入楼群时一般会考虑这一点，主要是为避免因雷击或与高压线接触而给人和设备安全带来的损失。建筑群子系统布线方式有以下几种：地下管道敷设方式、直埋沟内敷设方式和架空等。不同方式各有其优缺点。

11.2.1.3 布线距离

在进行结构化布线系统设计时，要注意线缆长度的限制。表 11.2 给出了 EIA/TIA-568 标准提出的布线距离最大值。

表 11.2 布线距离

m

子 系 统	光 纤	屏蔽双绞线	无屏蔽双绞线
建筑群(楼栋间)	2000	800	700
主干(设备间到配线间)	2000	800	700
配线间到工作区信息插座		90	90
信息插座到网卡		10	10

11.2.2　网络分析与设计过程

11.2.2.1　网络系统生命周期

一般来说，网络生命周期至少包括网络系统的构思和计划、分析和设计、运行和维护的过程。网络系统的生命周期是一个循环迭代的过程，每一个迭代周期都是网络重构的过程。常见的迭代周期构成方式主要有以下 3 种。

1. 四阶段周期

4 个阶段为：构思与规划阶段、分析与设计阶段、实施与构建阶段、运行与维护阶段。其特点是能够快速适应新的需求变化，工作成本低，适用于网络规模较小、需求较为明确、网络结构简单的网络工程。

2. 五阶段周期

这是一种较为常见的迭代周期划分方法，它将一次迭代划分成 5 个阶段：需求规范、通信规范、逻辑网络设计、物理网络设计、实施阶段。每个阶段都是一个工作环节，每个环节完毕后才能进入下一个环节，一般情况下不允许返回到前面的阶段。

3. 六阶段周期

六阶段周期是对五阶段周期的补充，分为需求分析、逻辑设计、物理设计、优化设计、实施及测试、检测及性能优化。

11.2.2.2　网络开发过程

根据五阶段迭代周期的模型，网络开发过程可以被划分为以下 5 个阶段。

1. 需求分析

需求分析是开发过程中最关键的阶段。不同的用户有不同的网络需求，收集的需求范围包括业务需求、用户需求、应用需求、计算机平台需求、网络通信需求，同时要考虑未来的需要，以便在以后对网络实现扩展。

需求分析的输出是产生一份需求说明，也就是需求规范。在写完需求说明书后，管理者和网络设计者应达成共识，并在文件上签字，这是规避网络建设风险的关键。

2. 现有网络系统的分析

如果网络开发过程是对现有网络的升级和改造，就必须进行现有网络系统的分析工作。现有网络系统分析的目的是描述资源分布，以便在升级时尽量保护已有的投资。

在这一阶段应给出一份正式的通信规范说明文档，作为下一阶段的输入。通信规范说明文档包括以下内容。

- 现有网络的拓扑结构。
- 现有网络的容量，以及新网络所需的通信量和通信模式。
- 详细的统计数据，直接反映现有网络性能的测量值。
- Internet 接口和广域网提供的服务质量报告。
- 限制因素列表，例如使用线缆和设备清单等。

3. 确定网络逻辑结构

网络逻辑结构设计是体现网络设计核心思想的关键阶段，在这一阶段根据需求规范和通信规范选择一种比较适宜的网络逻辑结构，并实施后续的资源分配规划、安全规划等内容。网络逻辑结构大致描述了设备的互连及分布范围，但是不确定具体的物理位置和运行环境。

这个阶段应得到一份逻辑设计文档，输出内容包括以下几点。

- 网络逻辑设计图。
- IP 地址分配方案。
- 安全管理方案。
- 具体的软硬件、广域网连接设备和基本的网络服务。
- 招聘和培训网络员工的具体说明。
- 对软硬件费用、服务提供费用以及员工和培训费用的初步估计。

4. 确定网络物理结构

物理网络设计是逻辑网络设计的具体实现，通过对设备的具体物理分布、运行环境等的确定来确保网络的物理连接符合逻辑设计的要求。

这一阶段应得到一份网络物理结构设计文档，输出的内容包括以下几点。

- 网络物理结构图和布线方案。
- 设备和部件的详细列表清单。
- 软硬件和安装费用的估算。
- 安装日程表，详细说明服务的时间以及期限。
- 安装后的测试计划。
- 用户的培训计划。

5. 安装和维护

安装是根据前面的工程结果实施环境准备、设备安装调试的过程。安装阶段的主要输出就是网络本身。网络安装完成后，接受用户的反馈意见和监控网络的运行是网络管理员的任务。

11.2.2.3　网络设计的约束因素

一般来说，网络设计的约束因素主要来自政策、预算、时间和应用目标等方面。

- 政策约束的具体表现是法律法规条文，以及国际、国家和行业标准等。
- 预算是决定网络设计的关键因素。网络预算一般分为一次性投资预算和周期性投资预算。一般来说，年度发送的周期性投资预算和一次性投资预算之间的比例为10%～15%比较合理。
- 项目进度表限定了项目最后的限期和重要的阶段。通常，项目进度由客户负责管理。
- 通过应用目标检查，可以避免用户需求的缺失，检查形式包括设计小组内的自我检查和用户主管部门的确认检查两种。

11.2.3　网络需求分析

网络需求分析是网络开发过程的起始部分，这一阶段应明确客户所需的网络服务和网络性能。

在需求分析过程中，需要考虑以下几个方面的需求：业务需求、用户需求、应用需求、计算机平台需求、网络需求。

11.2.3.1　业务需求

网络系统是为一个集体提供服务的，对于该集体内的不同用户，需要收集特定的业务信息，包括以下几个方面。

- 确定结构组织。业务需求的第一步就是获取组织机构图，了解集体中的岗位设置以及岗位职责。
- 确定关键时间点。对于大型项目，必须制订严格的项目实施计划，确定各个阶段关键的时间点。
- 确定网络投资规模。在整个网络的设计和实施中，费用是一个主要考虑的因素。
- 确定业务活动。主要通过对业务的分析，形成各类业务的网络需求，主要包括最大用户数、并发用户数、峰值带宽和正常带宽等。
- 预测增长率。通过对网络发展趋势的分析，明确网络的伸缩性需求。
- 确定网络的可靠性和可用性。网络设计人员在进行需求分析的过程中，首先应获取行业的网络可靠性和可用性标准，并根据标准与用户进行交流，确定特殊的要求。
- 确定 Web 站点和 Internet 连接。
- 确定网络的安全性。
- 确定远程接入方式。

11.2.3.2　用户需求

收集用户需求是要找出用户需要的重要服务和功能。收集用户需求的机制主要包括与用户群的交流、用户服务和需求归档 3 个方面。

收集用户需求最常用的方式有：观察和问卷调查、集中访谈、采访关键人物。在整个设计和实施阶段，应始终保持与关键人员之间的交流，以确保网络工程建设不偏离用户需求。

用户服务表用于表示收集和归档的需求信息，也用来指导管理人员和网络用户进行讨论。

11.2.3.3　应用需求

收集应用需求可以从两个角度出发：应用类型和应用对资源访问。

应用类型可分为以下几种。

- 按功能对应用进行分类，可以将应用划分为常见功能类型和特定功能类型。
- 按共享分类，可以将应用分为单用户软件、多用户软件和网络软件。
- 按响应方式，应用可以分为实时和非实时两种。
- 按网络规模，应用分为单机软件、对等网络软件、C/S 软件、BPS 软件和分布式软件等。

用户对网络资源的访问，是可以通过各种指标进行量化的，需要考虑的指标包括：每个应用的用户数量、每个用户平均使用每个应用的频率、使用高峰期、平均访问时间长度、每个事务的平均大小、每次传输的平均通信量和影响通信的定向特性。

11.2.3.4 计算机平台需求

需要调查的计算机平台主要有个人计算机、工作站、小型机、中型机和大型机。

这一阶段的输出是计算机平台需求表，它是总结用户对计算机平台需求的表格。

11.2.3.5 网络需求

需求分析的最后工作是考虑网络管理员的需求，包括以下内容。

- 局域网功能。对于升级的网络，可以对现有网段划分方式进行改进，形成新的划分方案。对于新建的网络，要和网络管理员一起商量网段的划分方式。
- 网络性能。主要考虑的是网络容量和响应时间。
- 有效性需求。有效性条件没有固定的模式，通常要对局域网的拓扑结构、网络设备、服务器主机、存储设备、安全设备、机房设备和产品供应商等设定一些选择标准或过滤条件。
- 数据备份和容灾中心需求。根据不同的网络工程规模，存在两种建设情况：一种是需要建设复杂的数据中心和容灾备份中心，另一种是仅建立数据备份和容灾机制。
- 网络管理需求。网络管理建设要从网络管理目的、网络管理要素、要管理的网络资源、软件资源管理和软件分发、应用管理等几个方面进行调查。
- 网络安全需求。安全技术措施包括机房及物理线路安全、网络安全、系统安全、应用安全、安全信任体系等。
- 城域网/广域网的选择。可供选择的连接方案有两种：点对点线路交换服务和分组交换服务。

11.2.3.6 编制需求说明书

编写需求说明书的目的是能够向管理人员提供决策用的信息，因此需求说明书应该做到尽量简明且信息充分。

对网络需求说明书存在两点要求。首先，无论需求说明书的组织形式如何，都应包含业务、用户、应用、计算机平台和网络 5 个方面的需求内容。其次，为了规范需求说明书的编制，一般情况下，需求说明书应该包括以下 5 个部分。

- 综述。
- 需求分析阶段总结。
- 需求数据总结。
- 按优先级排队的需求清单。
- 申请批准部分。

11.2.4 通信流量分析

通信规范分析最终的目标是产生通信流量，其中必要的工作是分析网络中信息流量的



分布问题。

11.2.4.1　通信流量分析的方法

80/20 规则是传统网络中广泛应用的一般规则。80/20 规则是基于这样的可能性：通信流量的 80%是在某个网段中流动，只有 20%的通信流量访问其他网段。80/20 规则适用于内部交流较多、外部访问相对较少、网络较为简单、不存在特殊应用的网络或网段。

但现在的网络，由于应用多样、资源分布分散等特性，使 80/20 规则出现翻转，即 80%的流量分配给远程，20%的流量在本地。这些需要根据网络业务特性进行决定。

11.2.4.2　通信流量分析的步骤

分析通信流量的具体步骤如下。

(1) 把网络分成易管理的网段。网段划分要考虑用户的需求，一般情况是按工作组或部分来划分网段。由于网段属于局域网络范畴，在进行分析工作前，需要确定网段的局域网通信边界。如果网段的通信边界是物理边界，则这个网段需要独立进行分析；如果多个网段的通信边界是逻辑边界，则这些网段不需要独立进行分析，而是作为一个整体网段来进行分析。

无论是物理网段分析，还是多个虚拟网段构成的整体网段分析，都可以采用局部分析法。局部分析法的实质在于只关注一个网段，并将网段边界外的其他部分等同于一个外部网络来进行分析。

(2) 确定个人用户和网段的通信量。这个步骤的工作在于将需求分析中不同格式的统计表格转化为统一的流量表格，以便于开始后续的分析工作。

(3) 确定本地和远程网段上通信流量的分布。这个步骤的重要任务是明确多少通信流量存在于网络内部，多少通信流量是访问其他网段。

(4) 对每个网段重复上述步骤。

(5) 分析广域网和网络骨干的通信流量。通信流量计算完成后，要把它们整理总结成一份文件，该文件将成为最终的通信规范说明书的一部分。

11.2.5　逻辑网络设计

逻辑网络设计过程主要由 4 个步骤组成：确定逻辑网络设计目标、网络服务评价、技术选项评价、进行技术决策。

11.2.5.1　逻辑网络设计目标

一般情况下，逻辑网络设计的目标如下。

- 合适的应用运行环境。
- 成熟稳定的技术选型。
- 合理的网络结构。
- 合适的运营成本。
- 逻辑网络的可扩充性能。
- 逻辑网络的易用性。
- 逻辑网络的可管理性。

● 逻辑网络的安全性。

11.2.5.2 需要关注的问题

(1) 设计要素：包括用户需求、设计限制、现有网络、设计目标。

(2) 设计面临的冲突：设计目标是一个复杂的整体，由不同维度的子目标构成，这些子目标之间可能存在冲突。

(3) 成本与性能：成本与性能是最常见的冲突目标，一般来说，网络设计方案的性能越高，也就意味着更高的成本，包括建设成本和运行成本。

11.2.5.3 主要的网络服务

对于大多数网络来说，都存在着两个主要的网络服务——网络管理和网络安全。

1. 网络管理

网络管理的重点内容是网络故障诊断、网络的配置及重配置和网络监视。

2. 网络安全

网络安全系统是网络逻辑设计的固有部分，可以采用以下步骤进行安全设计。

(1) 明确需要安全保护的系统。

(2) 确定潜在的网络弱点和漏洞。

(3) 尽量简化安全。

(4) 制定安全制度。

11.2.5.4 技术评价

在进行正确的网络技术选择时，应该考虑通信带宽、技术成熟性、连接服务类型、可扩充性、高投资产出比等因素。

11.2.5.5 逻辑网络设计的工作内容

逻辑网络设计的工作内容主要有网络结构的设计、物理层技术选择、局域网技术选择与应用、广域网技术选择与应用、地址设计和命名模型、路由选择协议、网络管理、网络安全和逻辑网络设计文档，并根据这些设计选择设备和服务供应商。

11.2.6 网络结构设计

网络结构是对网络进行逻辑抽象，描述网络中主要连接设备和网络计算机节点分布而形成的网络主体框架，不同于网络拓扑结构。由于当前的网络工程主要由局域网和实现局域网互连的广域网构成，因此可以将网络工程中的网络结构设计分成局域网结构和广域网结构两个设计部分。局域网结构主要讨论链路层的设备互连方式，而广域网结构主要讨论网络层的互连方式。

11.2.6.1 局域网结构

1. 单核心局域网结构

单核心局域网结构主要由一台核心二层或三层交换设备构建局域网的核心，通过多台



接入交换机接入计算机节点，该网络一般通过与核心交换机互连的路由设备接入广域网，如图 11.1 所示。

2. 双核心局域网结构

双核心局域网结构主要由两台核心交换设备构建局域网的核心，该网络一般也是通过与核心交换机互连的路由设备接入广域网，并且路由器与两台核心交换设备之间都存在物理链路，如图 11.2 所示。

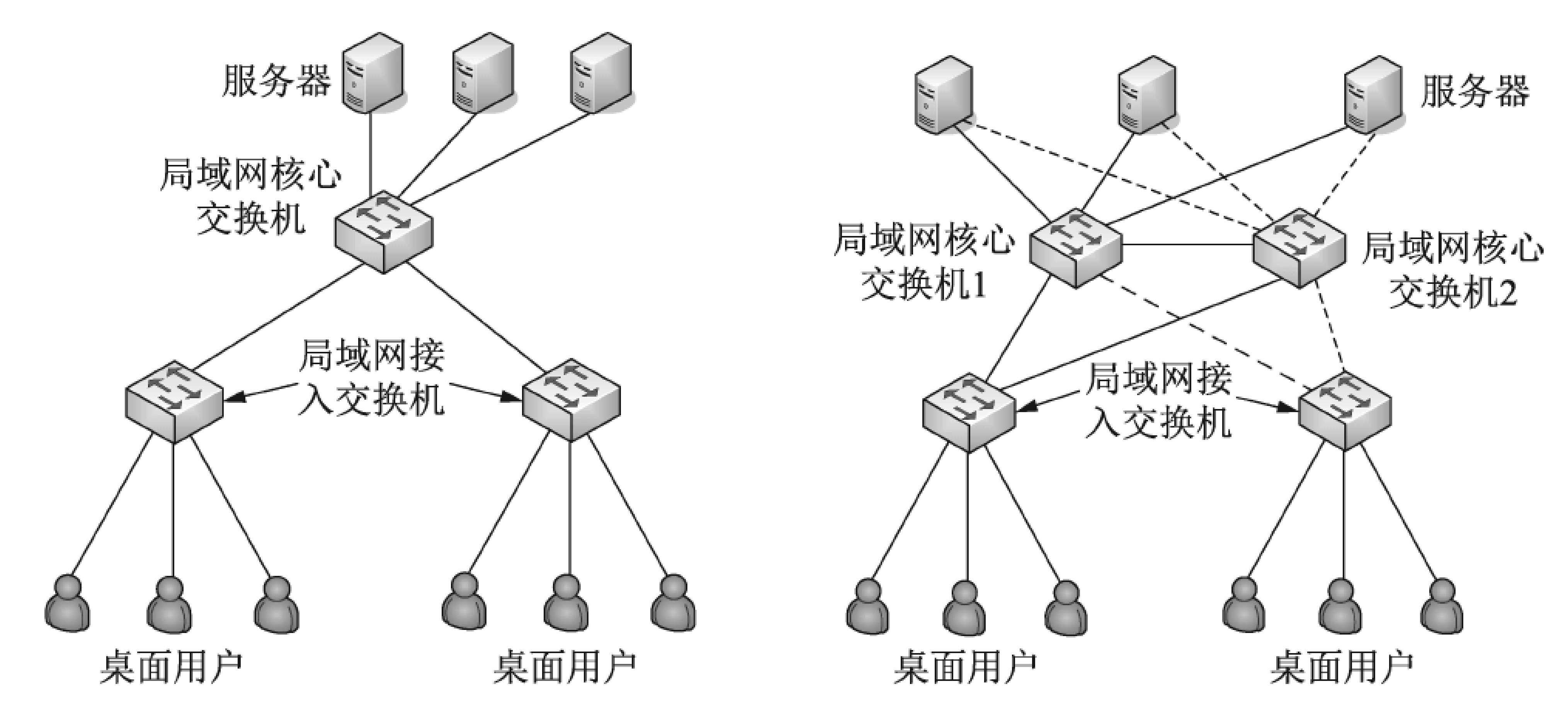


图 11.1　单核心局域网结构　　　　图 11.2　双核心局域网结构

3. 环型局域网结构

环型局域网结构由多台核心三层设备连接成双 RPR 动态弹性分组环，构成整个局域网络的核心，该网络通过与环上交换设备互连的路由设备接入广域网，如图 11.3 所示。

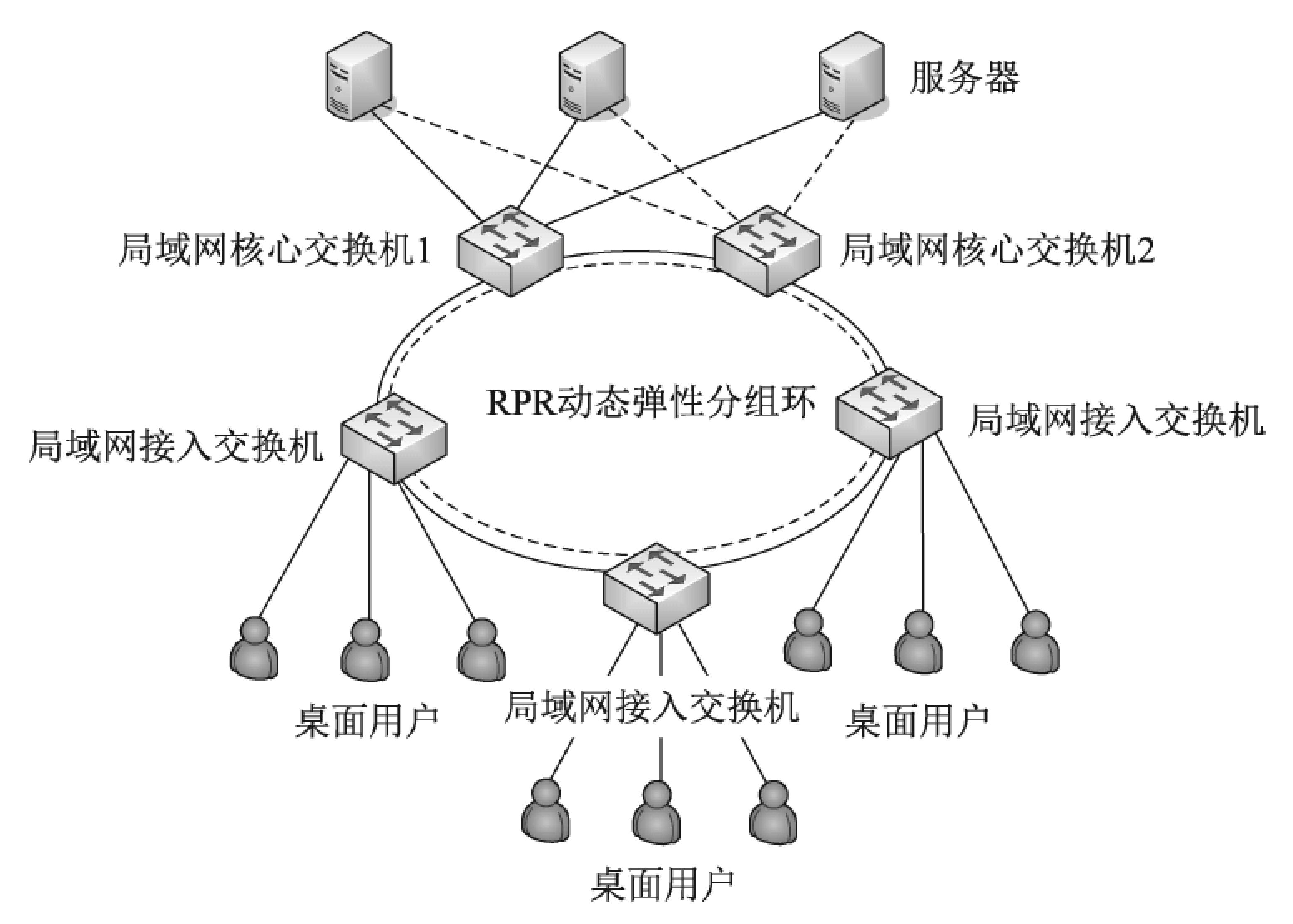


图 11.3　环型局域网结构

4. 层次局域网结构

层次结构主要定义了根据功能要求不同将局域网络划分层次构建的方式，从功能上定

义了核心层、汇聚层和接入层。层次局域网一般通过与核心层设备互连的路由设备接入广域网，如图11.4所示。

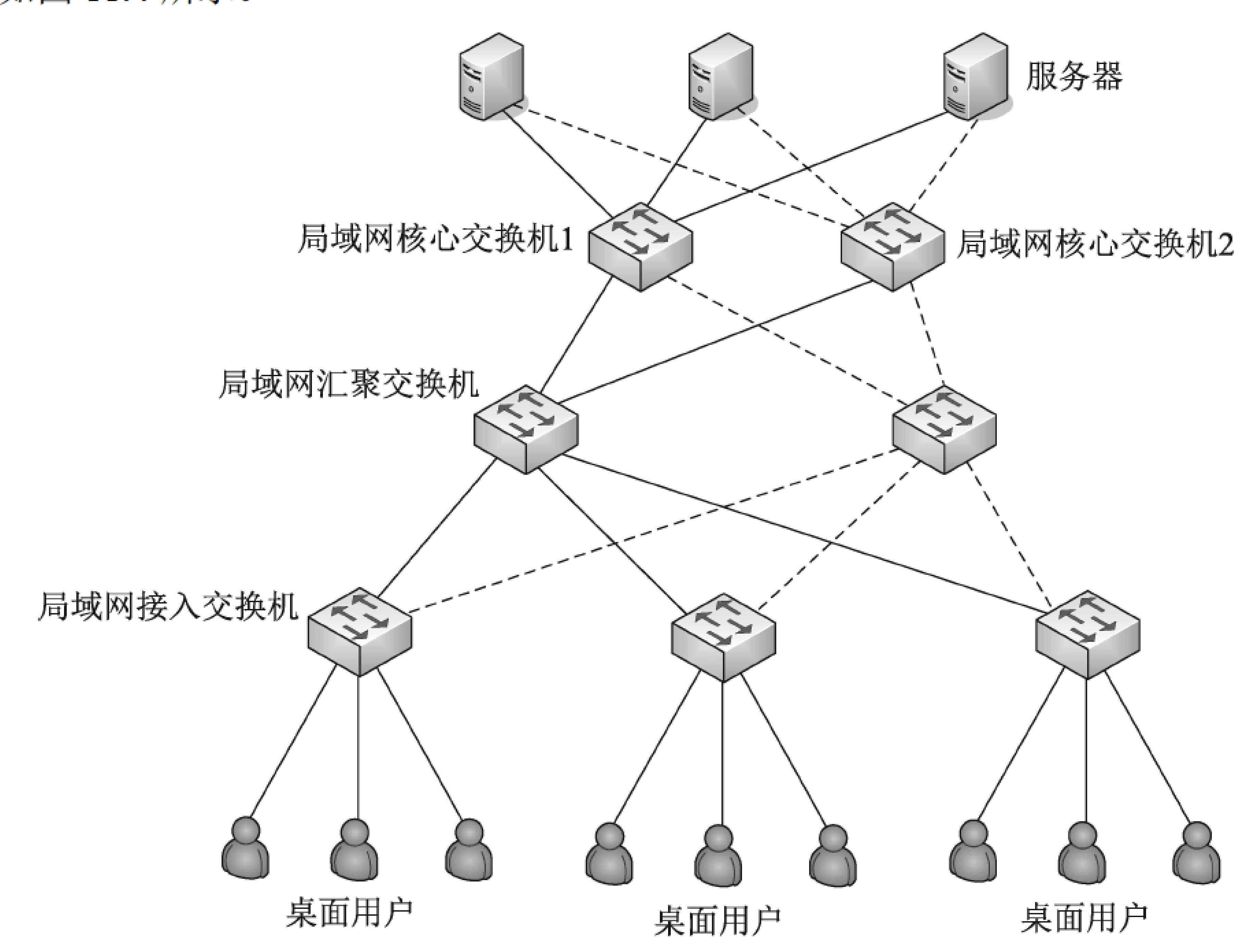


图 11.4 层次局域网结构

11.2.6.2 层次化网络设计

1. 层次化网络设计模型

层次化网络设计模型已经成为网络主流的园区网络的经典模型。一个典型的层次化网络结构应具有以下部分。

- 由经过可用性和性能优化的高端路由器和交换机组成的核心层。
- 由用于实现策略的路由器和交换机构成的汇聚层。
- 通过用以连接用户的低端交换机等构成的接入层。

2. 三层模型

层次化模型中最为经典的是三层模型。三层模型主要将网络划分为核心层、汇聚层和访问层。

- 核心层：提供不同区域或者下层的高速连接和最优传输路径。
- 汇聚层：将网络业务连接到接入层，并且实施与安全、流量负载和路由相关的策略。
- 访问层：为局域网接入广域网或者终端用户访问网络提供接入。

1) 核心层设计要点

核心层是网络高速交换的主干，对整个网络的性能至关重要，因此在设计中应该采用冗余组件设计，使其具备高可靠性，能够快速适应变化。在设计核心层设备的功能时，应尽量避免使用数据包过滤、策略路由等降低数据包转发处理的机制，以优化核心层获得低



延迟和良好的可管理性。

2) 汇聚层设计要点

汇聚层处于核心层与接入层的分界点，应尽量将出于安全性原因对资源访问的控制、出于性能原因对通过核心层流量的控制等都在汇聚层实施。

为了保证层次化的特性，汇聚层应该向核心层隐藏接入层的详细信息。另外，汇聚层也会对接入层屏蔽网络其他部分的信息。为了保证核心层连接运行不同协议的区域，各种协议的转换都应在汇聚层完成。

3) 接入层设计要点

接入层为用户提供了在本地网段访问应用系统的能力，接入层要解决相邻用户之间的互访需要，并且为这些访问提供足够的带宽。接入层还要负责一些用户管理功能和用户信息收集工作。

11.2.6.3　设备选择

1. 主要指标

- 设备档次：可以根据网络的拓扑对各层设备作先期的选型估计，最能确定设备档次的是性能要求，其次是接口类型、各层设备接口数、可靠性要求。
- 接口类型、数量：具体的接口类型取决于用户选用的线路。而线路的选择则取决于网络的数据流量的估算、当地各种线路的性价比。具体的接口数量取决于整个网络的节点数、接口类型、带宽等一系列的综合结构。
- 可靠性要求：是否需要主控冗余备份、电源冗余备份、接口备份、设备间备份等。
- 特殊应用数据采集：是否有 VoIP 的需求，各级 IP 语音接口的 CALL 数峰值。这也将是设备选择中的重要内容。

2. 选择依据——网络数据采集

- 带宽数据：计算所有业务每秒钟所需的平均带宽。
- 接口类型、数量：根据现有的网络结构、需要建设的网络拓扑、网络线路选择情况，确定各层设备需要选择的网络接口类型和接口数量。
- 性能数据：根据线路情况、带宽情况，可以确定各层设备对性能的要求。
- 特殊应用数据采集：是否有 VoIP 的需求，各级 IP 语音接口的 CALL 数峰值。

3. 网络设备层次选择原理

- 广域网和局域网分开。
- 局域网、广域网分层设计。

4. 设备选择原则

- 设备档次主要由设备的网络位置来决定。
- 可靠性要求。
- 性能要求。
- 接口数量要求。
- 接口类型。

11.2.6.4 网络冗余设计

网络冗余设计是通过设置双重网络元素来满足网络的可用性需求，冗余降低了网络的单点失效，其目的是重复设置网络组件，以避免单个组件的失效而导致应用失效。

在网络冗余设计中，对于通信线路常见的设计目标主要有两个：一个是作为备用路径，另一个是负载分担。

1. 备用路径

备用路径主要是为了提高网络的可用性。当一条路径或者多条路径出现故障时，为了保障网络的连通，网络中必须存在冗余的备用路径。备用路径由路由器、交换机等设备之间的独立备用链路组成。一般情况下，备用路径仅仅在主路径失效时投入使用。

2. 负载分担

负载分担是通过冗余的形式来提高网络的性能，是对备用路径方式的补充。负载分担是通过并行链路提供流量分担来提高性能，其主要的实现方法是利用两个或多个网络接口和路径来同时传递流量。不同类型的拓扑结构具有不同的冗余性，在选择的时候应该注意。

- 星型结构简单，管理方便，但冗余性不好，中心压力大，存在单点故障。
- 树型结构简单，中心压力小，但冗余性也不好，且有单点故障。
- 环型结构简单，管理方便，投资小，具有一定冗余度，但在网络存在差异较大的路径时，会引起网络时延的剧烈变化。
- 网状拓扑结构具有最小的时延、最高的冗余可靠性，但管理复杂，造价非常昂贵，常用于广域网。

11.2.7 网络故障诊断

11.2.7.1 引发网络故障的原因及排除流程

网络故障诊断是以网络原理、网络配置和网络运行的知识为基础，从故障现象出发，以网络诊断工具为手段获取诊断信息、确定网络故障点、查找问题的根源、排除故障、恢复网络正常运行的过程。

1. 引发网络故障的原因

- 物理层中物理设备相互连接失败或者硬件及线路本身的问题。
- 数据链路层的网络设备的接口配置问题。
- 网络层网络协议配置或操作错误。
- 传输层的设备性能或通信拥塞问题。
- 上三层或网络应用程序错误。

2. 排除网络故障的流程

在排除网络中出现的故障时，使用系统的方法往往更为有效。系统的方法流程如下：定义特定的故障现象，根据特定现象推断出可能发生故障的所有潜在问题，直到故障现象不再出现为止。图11.5给出了一般故障排除模型的处理流程。



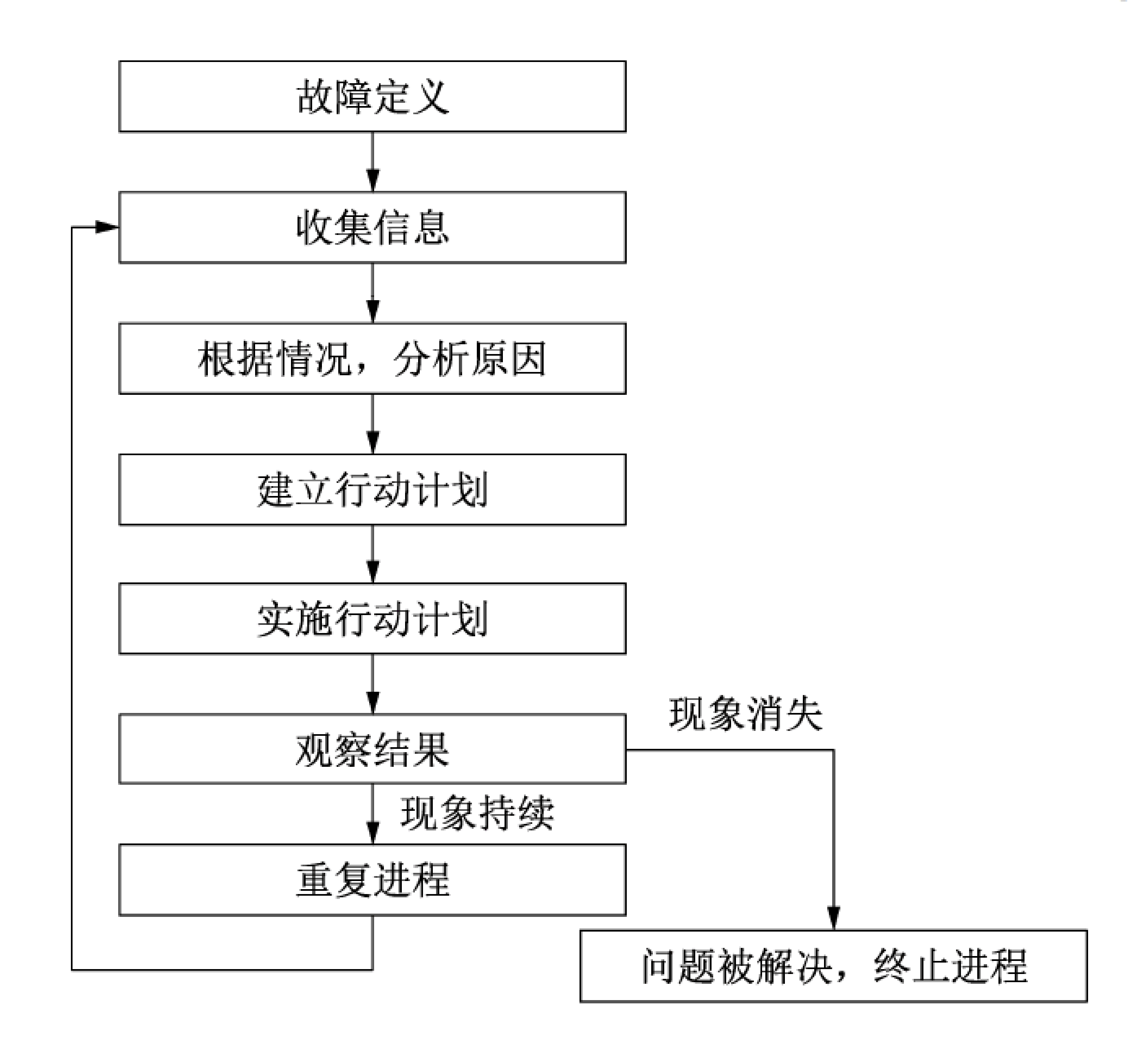


图 11.5　一般性故障问题的解决模型

注意：在网络故障的排除过程中，最为关键的是确保当前掌握的信息及资料是最新的。

11.2.7.2　网络故障排除工具

排除网络故障常用的工具有三类：设备或系统诊断命令、网络管理工具以及专业故障排除工具。

1. 设备或系统诊断命令

- show：用于监视系统的安装情况与网络的正常运行情况，也可用于对故障区域的定位。
- debug：帮助分离协议和配置问题。
- ping：用于检查网络上不同设备之间的连通性。
- trace：用于确定数据包从一个设备到另一个设备直至目的地的过程中所经历的路径。

2. 网络管理工具

Cisco Works、HP OpenView 等网络管理工具都含有监测以及故障排除功能。

3. 专业故障排除工具

- 欧姆表、数字万用表及电缆测试器。其中电缆测试器可用于检测电缆的物理连通性。
- 时域反射器与光时域反射器。时域反射器(TDR)能够快速地定位金属电缆中的短路、断路、压接、扭结、阻抗不匹配等问题；光时域反射器(OTDR)可以精确地测量光纤的长度、定位光纤的断裂处、测试光纤的信号衰减、测试接头或连接器造成的损耗。
- 断接盒、智能测试盘和位/数据块错误测试器。这类设备可以检测数据线路的状态，捕获并分析数据，诊断数据通信系统中常见的故障。

- 网络检测器。该设备可以收集诸如数据包长度、数据包数量、错误数据包的数据、连接的总体利用率、主机与 MAC 地址的数量等信息。网络检测器不会对数据帧中的内容进行解码。
- 网络分析仪。它能够对不同协议层的通信数据进行解码，以便于阅读的缩略语或概述形式表示出来，详细表示哪个层被调用，以及每个字节或者字节内容起什么作用。

11.2.7.3　网络故障分层诊断

根据网络故障的性质把网络故障分为物理故障(硬件故障)与逻辑故障(软件故障)，也可以根据网络故障的对象把网络故障分为线路故障、路由故障和主机故障。

1. 物理层及其诊断

物理层的故障主要表现在设备的物理连接方式是否恰当，连接电缆是否正确。确定路由器端口物理连接是否完好的最佳方式是使用 show interface 命令。

2. 数据链路层及其诊断

查找和排除数据链路层的故障，需要查看路由器的配置，检查连接端口共享同一数据链路层的封装情况。

3. 网络层及其诊断

排除网络层故障的基本方式是：沿着从源到目标的路径查看路由器的路由表，同时检查路由器接口的 IP 地址。

4. 应用层及其诊断

排除应用层故障的基本方法是：首先在服务器上检查配置，测试服务器是否正常运行，如果服务器没有问题再检查应用客户端是否正确配置。

11.3　真题详解

11.3.1　综合知识试题

试题 1　(2017 年下半年试题 64)

以下关于层次化网络设计的叙述中，错误的是__(64)__。

(64) A. 核心层实现数据分组从一个区域到另一个区域的高速转发
　　B. 接入层应提供丰富接口和多条路径来缓解通信瓶颈
　　C. 汇聚层提供接入层之间的互访
　　D. 汇聚层通常进行资源的访问控制

参考答案：(64)B。

要点解析：接入层为用户提供了在本地网段访问应用系统的能力，接入层要解决相邻用户直接的互访需要，并且为这些访问提供足够的带宽，并不考虑多路径选择。



试题 2　(2017 年上半年试题 47)

当传输介质出现老化、破损、介质规格不匹配时会导致物理接口处于 DOWN 状态，常使用__(47)__命令检查光纤模块状态、参数是否正常。

(47) A. virtual-cable-test　　B. display transceiver interface

C. display device　　D. display interface

参考答案：(47)B。

要点解析：display transceiver 用来显示设备接口上的光模块信息。

试题 3　(2017 年上半年试题 48 和试题 49)

在网络运行中，发现设备 CPU 长时间占用率过高，经检查发现图 11.6 中的"Number of to pology changes"值频繁变化，可初步判断该故障由__(48)__导致，可能的原因是__(49)__。

```
<Switch> display stp topology-change
                    CIST topology change information
Number of topology changes                 :35
Time since last topology change            :0 days 1h:7m:30s
Topology change initiator(notified)        :GigabitEthernet2/0/6
Topology change last received from         :101b-5498-d3e0
Number of generated topologychange traps:   38
Number of suppressed topologychange traps:   8
```

图 11.6　网络运行

(48) A. 硬件故障　　B. 网络攻击　　C. 网络震荡　　D. 网络环路

(49) A. 网络上某个端口链路属性频繁变化

B. 广播风暴造成大量协议报文

C. 设备受到 DHCP 协议报文攻击

D. 在部分硬件故障时会上报大量中断

参考答案：(48)C；(49)A。

要点解析：拓扑信息变动频繁，可以推测产生了网络震荡。出现网络震荡时，网络频繁变动，设备忙于处理网络切换事件，导致 CPU 占用率高。

试题 4　(2017 年上半年试题 50)

在 SwitchA 上 ping SwitchB 的地址 192.168.1.100 不通。通过步骤①到④解决了该故障，该故障产生的原因是__(50)__。

① 使用 display port vlan 命令查看 SwitchA 和 SwitchB 接口配置。

② 使用 display ip interfacebrief 命令查看 SwitchA 和 SwitchB 接口配置。

③ 使用 port link-type trunk 命令修改 SwitchB 接口配置。

④ 使用 ping 192.168.1.100 检查，故障排除。

(50) A. SwitchB 接口 VLAN 不正确

B. SwitchB 的接口状态为 DOWN

C. SwitchB 链路类型配置错误

D. SwitchB 对接收到的 ICMP 报文丢弃

参考答案：(50)C。

要点解析：由步骤③可知交换机 B 配置做出了修改，说明两边链路封装不一致。

试题 5 (2017 年上半年试题 67 和试题 68)

结构化综合布线系统分为六个子系统，其中水平子系统的作用是__(67)__，干线子系统的作用是__(68)__。

(67) A. 实现各楼层设备间子系统之间的互连
B. 实现中央主配线架和各种不同设备之间的连接
C. 连接干线子系统和用户工作区
D. 连接各个建筑物中的通信系统

(68) A. 实现各楼层设备间子系统之间的互连
B. 实现中央主配线架和各种不同设备之间的连接
C. 连接干线子系统和用户工作区
D. 连接各个建筑物中的通信系统

参考答案：(67)C；(68)A。

要点解析：水平子系统目的是实现信息插座和管理子系统(跳线架)之间的连接。干线子系统的作用是通过骨干线缆将主设备间和各楼层配线间体系连接起来。

试题 6 (2017 年上半年试题 69)

图 11.7 为某公司网络管理员规划的新办公大楼网络拓扑图，针对该网络规划，以下说法中不合理的是__(69)__。

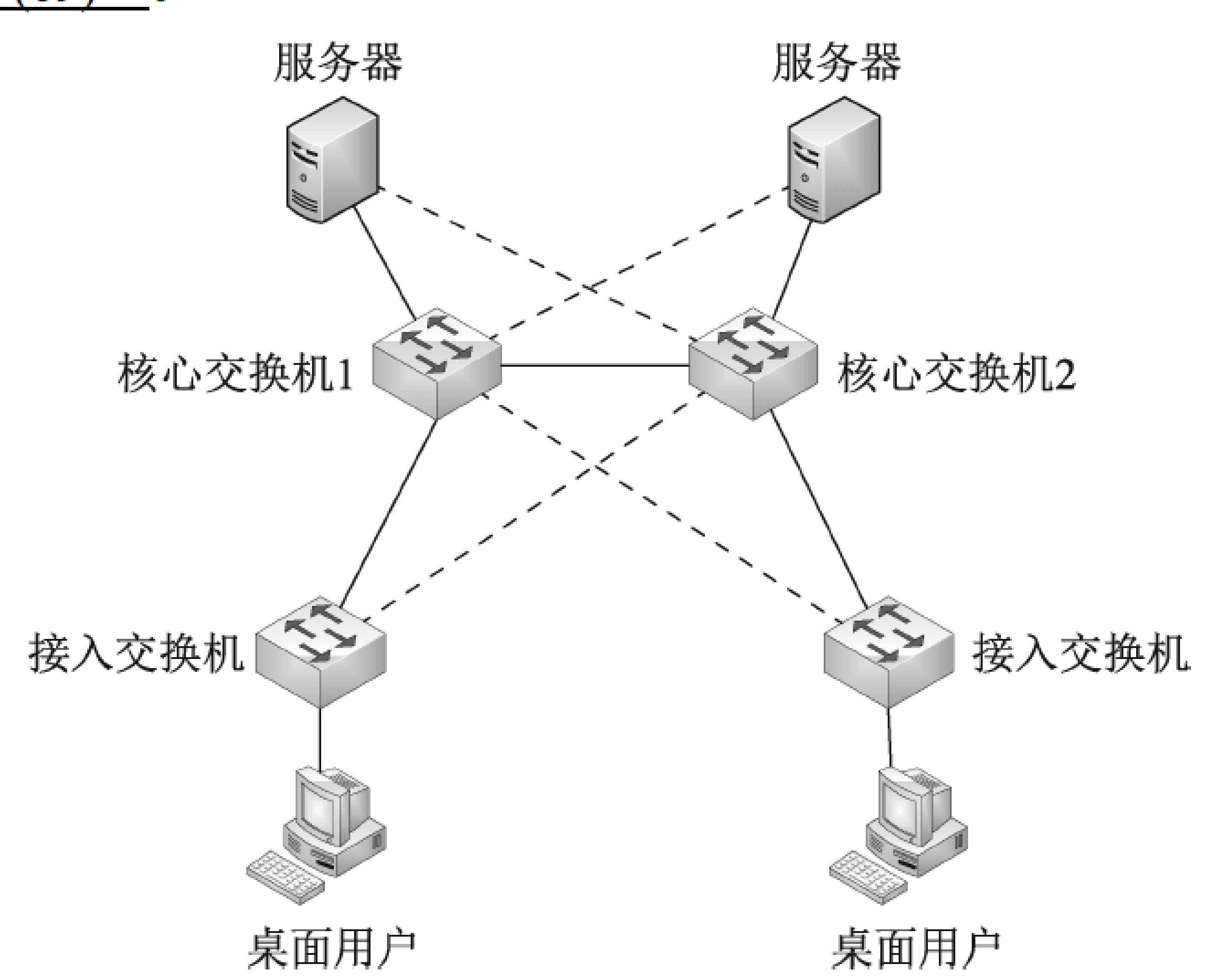
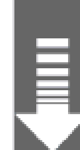


图 11.7 新办公楼网络拓扑图

(69) A. 核心交换机之间可以采用 VRRP、虚拟化等技术手段
B. 网络内各 VLAN 之间访问需要经过两台核心交换设备中的一台
C. 接入交换机多采用三层交换机
D. 网络拓扑结构可靠

参考答案：(69)C。



要点解析：接入层是网络中直接面向用户连接或访问的部分，所以接入层应提供种类丰富、数量多的端口，从而提供强大的接入功能，除此之外还要考虑接入的安全性问题。因此一般不采用三层交换机。

试题 7　(2017 年上半年试题 70)

在对网络设备巡检中，检测到交换机端口有大量的 CRC 错包(见图 11.8)，结合错包呈现出不断上涨的趋势，下面故障原因中，不可能的是__(70)__。

```
[Switch-GiagabitEthernet0/0/1]display this interface
GiagabitEthernet0/0/1 current state:UP
Line protocol current state:UP
Unicast   :  984907,Multicast  :  0
Broadcast :  0,Jumbo           :  0
CRC       :  4782,Giants       :  0
Jabbers   :  0,Throttles       :  0
Run ts    :  0,DropEvents      :  0
```

图 11.8　对网络设备巡检

(70) A. 端口状态异常　　B. 物理链路故障
C. 电磁干扰　　D. 病毒攻击

参考答案：(70)D。

要点解析：出现大量的 CRC 错包，说明是网络底层的相应故障，不可能是病毒攻击。

试题 8　(2016 年下半年试题 29)

结构化布线系统分为六个子系统，其中干线子系统的作用是__(29)__。

(29) A. 连接各个建筑物中的通信系统
B. 连接干线子系统和用户工作区
C. 实现中央主配线架与各种不同设备之间的连接
D. 实现各楼层设备间子系统之间的互连

参考答案：(29)D。

要点解析：干线子系统是结构化综合布线系统中连接各管理间、设备间的子系统，又称垂直子系统。

试题 9　(2016 年下半年试题 68)

在网络设计和实施过程中要采取多种安全措施，下面的选项中属于系统安全需求措施的是__(68)__。

(68) A. 设备防雷击　　B. 入侵检测
C. 漏洞发现与补丁管理　　D. 流量控制

参考答案：(68)C。

要点解析：设备防雷击属于机房及物理线路安全需求；入侵检测、流量控制属于网络安全需求；漏洞发现与补丁管理属于系统安全需求。

试题 10　(2016 年下半年试题 69)

在网络的分层设计模型中，对核心层工作规程的建议是__(69)__。

(69) A. 要进行数据压缩以提高链路利用率
B. 尽量避免使用访问控制列表以减少转发延迟
C. 可以允许最终用户直接访问
D. 尽量避免冗余连接

参考答案：(69)B。

要点解析：核心层是网络高速交换的主干，对整个网络的性能至关重要，设计时应采用冗余组件设计，使其具备高可靠性，快速适应变化。设计核心层设备的功能时，应尽量避免使用数据包过滤、策略路由等降低数据包转发处理的机制，以优化核心层获得低延迟和良好的可管理性。

试题 11 (2016 年下半年试题 70)

在网络规划和设计过程中，选择网络技术时要考虑多种因素。下面的各种考虑中不正确的是__(70)__。

(70) A. 网络带宽要保证用户能够快速访问网络资源
B. 要选择具有前瞻性的网络新技术
C. 选择网络技术时要考虑未来网络扩充的需求
D. 通过投入产出分析确定使用何种技术

参考答案：(70)B。

要点解析：在进行正确的网络技术选择时，应该考虑：通信带宽、技术成熟性、连接服务类型、可扩充性、高投资产出比等因素。有些新的应用技术在尚未大规模投入应用时，还存在着较多不确定因素，而这些不确定因素将会为网络建设带来很多不可估量的损失。虽然新技术的自身发展离不开工程应用，但是对于大型网络工程来说，项目本身不能成为新技术的试验田。因此，尽量使用较为成熟、拥有较多案例的技术是明智的选择。

试题 12 (2016 年上半年试题 68)

在网络中分配 IP 地址可以采用静态地址或动态地址方案。下面关于两种地址分配方案的论述中错误的是__(68)__。

(68) A. 采用动态地址分配方案可避免地址资源的浪费
B. 路由器、交换机等联网设备适合采用静态 IP 地址
C. 各种服务器设备适合采用动态 IP 地址分配方案
D. 学生客户机最好采用动态 IP 地址

参考答案：(68)C。

要点解析：在网络中分配 IP 地址可以采用静态地址或动态地址方案，各种服务器设备适合采用静态 IP 地址分配方案，方便管理和做域名解析。学生客户机 PC 开机使用时，分配 IP 地址，关机时释放 IP 地址。

试题 13 (2016 年上半年试题 69 和试题 70)

网络设计过程包括逻辑网络设计和物理网络设计两个阶段，各个阶段都要产生相应的文档。下面的选项中，属于逻辑网络设计文档的是__(69)__，属于物理网络设计文档的是__(70)__。

(69) A. 网络 IP 地址分配方案　　B. 设备列表清单
C. 集中访谈的信息资料　　D. 网络内部的通信流量分布
(70) A. 网络 IP 地址分配方案　　B. 设备列表清单
C. 集中访谈的信息资料　　D. 网络内部的通信流量分布

参考答案：(69)A；(70)B。

要点解析：逻辑网络设计的任务是根据需求规范和通信规范，实施资源分配和安全规划。主要包括：层次网络结构设计；物理层技术选择；局域网技术选择与应用；广域网技术选择与应用；地址设计与命名模型；路由选择协议；网络管理；网络安全；逻辑网络设计文档。

物理网络设计的任务是设计特定的物理环境平台，主要包括结构化综合布线系统的设计，机房环境设计，传输介质和网络设备选型及安装方案，特殊设备安装方案和网络实施等。

试题 14　(2015 年下半年试题 48)

某用户无法访问域名为 www.cisco.com 的网站，在用户主机上执行 tracert 命令得到提示如下：

```
Tracing route to www.cisco.com[119.188.155.27]
Over amaximum of 30 hops:
1   <1ms   <1ms   <1ms   202.117.112.129
2   202.117.112.129   report: Destination net unreachable
```

根据提示信息，造成这种现象的原因可能是__(48)__。

(48) A. 用户主机的网关设置错误
B. 用户主机设置的 DNS 服务器工作不正常
C. 路由器上进行了相关 ACL 设置
D. 用户主机的 IP 地址设置错误

参考答案：(48)C。

要点解析：tracert(跟踪路由)是路由跟踪实用程序，用于确定 IP 数据包访问目标所采取的路径。

试题 15　(2015 年下半年试题 68 和试题 69)

通过 HFC 网络实现宽带接入，用户端需要的设备是__(68)__，终端用于控制和管理用户的设备是__(69)__。

(68) A. Cable Modem　　B. ADSL Modem
C. OLT　　D. CMTS
(69) A. Cable Modem　　B. ADSL Modem
C. OLT　　D. CMTS

参考答案：(68)A；(69)D。

要点解析：HFC 是将光缆敷设到小区，然后通过光电转换节点，利用有线电视 CATV 的总线式同轴电缆连接到用户，提供综合电信业务的技术。这种方式可以充分利用 CATV 原有的网络，建网快、造价低，逐渐成为最佳的接入方式之一。HFC 是由光纤干线网和同

轴电缆分配网通过光节点站结合而成的，一般光纤干线网采用星型拓扑，同轴电缆分配网采用树型结构。

在同轴电缆的技术方案中，用户端需要使用一个称为 Cable Modem(电缆调制解调器)的设备，它不单纯是一个调制解调器，还集成了调谐器、加/解密设备、桥接器、网络接口卡、虚拟专网代理和以太网集线器的功能于一身，它无须拨号，可提供随时在线的永久连接。其上行速率已达 10Mb/s 以上，下行速率更高。

CMTS(电缆调制解调器终端系统)是管理控制 Cable Modem 的设备，其配置可通过 Console 接口或以太网接口完成。其配置内容主要有：下行频率、下行调制方式、下行电平等。

试题 16 (2015 年下半年试题 70)

以下关于层次化局域网模型中核心层的叙述，正确的是 __(70)__。

(70) A. 为了保障安全性，对分组要进行有效性检查
B. 将分组从一个区域高速地转发到另一个区域
C. 由多台二、三层交换机组成
D. 提供多条路径来缓解通信瓶颈

参考答案：(70)B。

要点解析：层次化模型中最为经典的是三层模型，主要将网络划分为核心层、汇聚层和接入层。核心层一般由经过可用性和性能优化的高端路由器和交换机组成，提供不同区域或者下层的高速连接和最优传送路径；汇聚层由用于实现策略的路由器或者交换机构成，将网络业务连接到接入层，并且实施与安全、流量负载和路由相关的策略；接入层由连接用户的低端交换机构成，为局域网接入广域网或者终端用户访问网络提供接入。

11.3.2 案例分析试题

试题 1 (2017 年下半年下午试题二)

【说明】

图 11.9 是某企业网络拓扑，网络区域分为办公区域、服务器区域和数据区域，线上商城系统为公司提供产品在线销售服务。公司网络保障部负责员工办公电脑和线上商城的技术支持和保障工作。

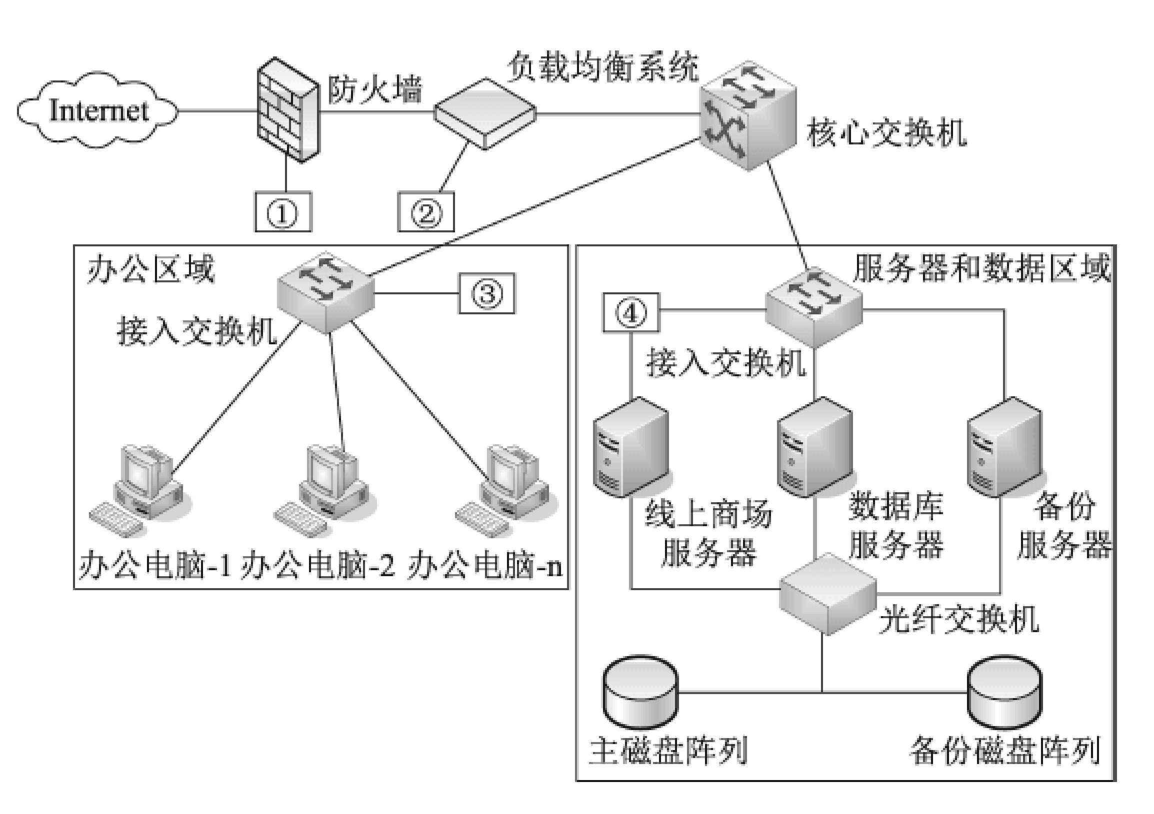


图 11.9 某企业网络拓扑



【问题 1】(6 分)

某天，公司有一台电脑感染“勒索”病毒，网络管理员应采取__(1)__、__(2)__、__(3)__措施。

(1)～(3)备选答案：

A. 断开已感染主机的网络连接

B. 更改被感染文件的扩展名

C. 为其他电脑升级系统漏洞补丁

D. 网络层禁止 135/137/139/445 端口的 TCP 连接

E. 删除已感染病毒的文件

【问题 2】(8 分)

图 11.8 中，为提高线上商城的并发能力，公司计划增加两台服务器，三台服务器同时对外提供服务，通过在图中__(4)__设备上执行__(5)__策略，可以将外部用户的访问负载平均分配到三台服务器上。

(5)备选答案：

A. 散列　　B. 轮询　　C. 最少连接　　D. 工作-备份

其中一台服务器的 IP 地址为 192.168.20.5/27，请将配置代码补充完整。

ifcfg-eml 配置片段如下：

```
DEVICE =eml
TYPE=Ethernet
UUID=36878246-2a99-43b4-81df-2db1228eea4b
ONBOOT=yes
NM_CONTROLLED=yes
BOOTPROTO=none
HWADDR=90:B1:1C:51:F8:25
IPADDR=192.168.20.5
NETMASK=__(6)__
GATEWAY=192.168.20.30
DEFROUTE= yes
IPV4_FAILURE_FATAL=yes
IPV6INTI=no
```

配置完成后，执行 systemct1__(7)__network 命令重启服务。

【问题 3】(4 分)

网络管理员发现线上商城系统总是受到 SQL 注入、跨站脚本等攻击，公司计划购置__(8)__设备/系统，加强防范；该设备应部署在图 11.9 中设备①～④的__(9)__处。

(8)备选答案：

A. 杀毒软件　　B. 主机加固

C. WAF(Web 应用防护系统)　　D. 漏洞扫描

【问题 4】(2 分)

图 11.9 中，存储域网络采用的是__(10)__网络。

参考答案：

【问题 1】(1)A；(2)C；(3)D。

【问题 2】(4)负载均衡系统；(5)B；(6)255.255.255.224；(7)restart。

【问题 3】(8)C；(9)④。

【问题 4】(10)FC-SAN。

要点解析：

【问题 1】

“勒索”病毒利用的是 Windows 系统漏洞，通过系统默认开发 135、137、445 等文件共享端口发起的病毒攻击，因此应该先将感染的主机断开网络连接，然后将其他主机也断开连接，并禁止共享操作，然后升级操作系统漏洞补丁，避免再次遭受攻击。

【问题 2】

实现负载均衡可直接在此网络上的负载均衡设备实现，并执行轮询设置，这样可实现对各服务器的负载均衡操作。由题可知服务器的 IP 地址为 192.168.20.5/27，因此可知子网掩码为 255.255.255.244，重启服务器的命令为：systemctl restart network。

【问题 3】

Web 应用防护系统，简称 WAF。Web 应用防火墙是执行一系列针对 HTTP/HTTPS 的安全策略来专门为 Web 应用提供保护的一种产品。它能够有效发现及阻止 SQL 注入，网页篡改，跨站脚本等攻击。其主要对服务器区域进行检测和保护，故放入④处最为适宜。

【问题 4】

存储网络，采用光纤连接存储区域，实现高速存储访问，符合 FC-SAN 支持块级调用，适合为大型数据库提供存储服务。

试题 2 (2017 年上半年下午试题一)

【说明】

某企业网络拓扑如图 11.10 所示，中国电信和中国移动双链路接入，采用硬件设备实现链路负载均衡：主磁盘阵列的数据通过备份服务器到备份磁盘阵列。请结合下图，回答相关问题。

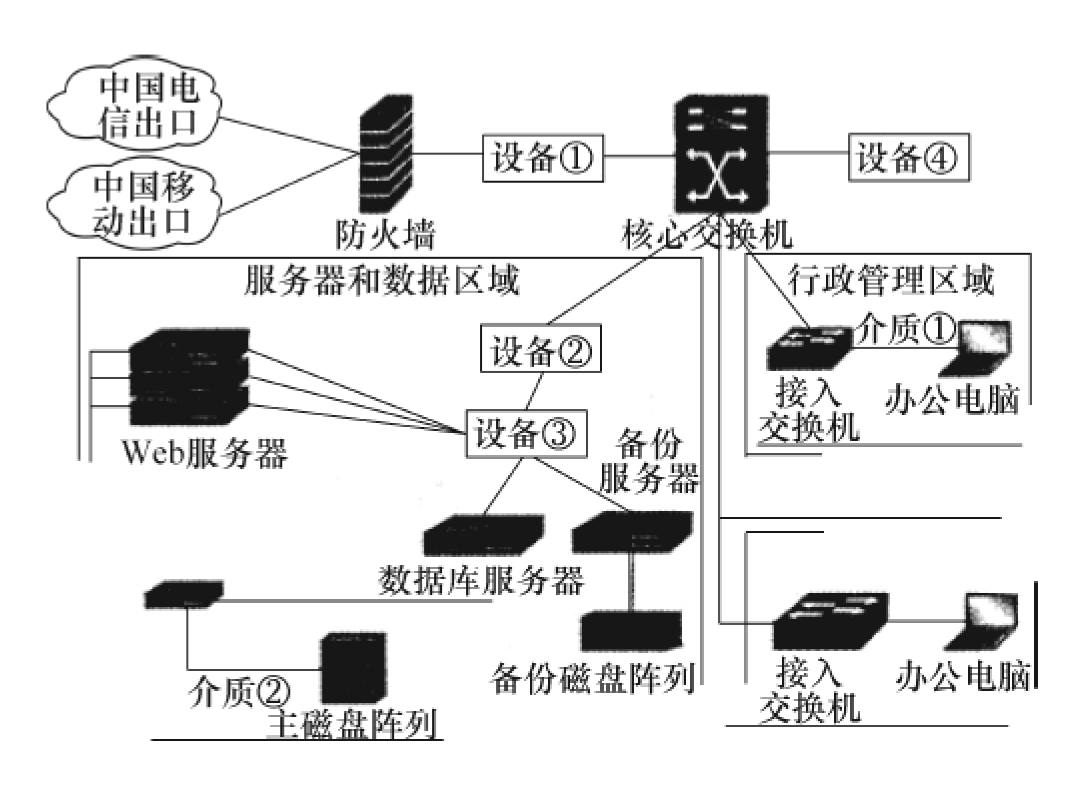


图 11.10　某企业网络拓扑

【问题 1】(共 6 分)

图 11.10 中，设备①处部署__(1)__，设备②处部署__(2)__，设备③处部署__(3)__。

(1)～(3)备选答案(每个选项限选一次)：

A. 入侵防御系统(IPS)　　B. 交换机　　C. 负载均衡





【问题 2】(共 4 分)

图 11.10 中，介质①处应采用__(4)__，介质②处应采用__(5)__。

(4)、(5)备选答案(每个选项限选一次):

A. 双绞线　　B. 同轴电缆　　C. 光纤

【问题 3】(共 4 分)

图 11.10 中，为提升员工的互联网访问速度，通过电信出口访问电信网络，移动出口访问移动网络，则需要配置基于__(6)__地址的策略路由；运行一段时间后，网络管理员发现电信出口的用户在 90%以上，网络访问速度缓慢，为实现负载均衡，网络管理员配置基于__(7)__地址的策略路由，服务器和数据区域访问互联网使用电信出口，行政管理区域员工访问互联网使用移动出口，生产业务区域员工使用电信出口。

【问题 4】(共 6 分)

1. 图 11.10 中，设备④处应为__(8)__，该设备可对指定计算机系统进行安全脆弱性扫描和检测，发现其安全漏洞，客观评估网络风险等级。

2. 图 11.10 中，__(9)__设备可对恶意网络行为进行安全检测和分析。

3. 图 11.10 中，__(10)__设备可实现内部网络和外部网络之间的边界防护，依据访问规则，允许或者限制数据传输。

参考答案：

【问题 1】(1)C；(2)A；(3)B。

【问题 2】(4)A；(5)C。

【问题 3】(6)目的；(7)源。

【问题 4】(8)漏洞扫描设备；(9)IPS；(10)防火墙。

要点解析：

【问题 1】

综合分析可知设备 3 是交换机，那么设备 2 为 IPS，设备 1 为负载均衡。

【问题 2】

介质 1 连接接入交换机和用户，故为双绞线。介质 2 连接 FC 交换机和磁盘阵列，应为光纤。

【问题 3】

访问电信网络通过电信出口，移动网络通过移动出口，这是通过访问目的来区分的，故是基于目的地址的策略路由。而后根据访问人群的划分更改为基于源地址的策略路由。

【问题 4】

漏洞扫描通常是指基于漏洞数据库，通过扫描等手段，对指定的远程或者本地计算机系统的安全脆弱性进行检查，发现可利用的漏洞的一种安全性检测行为。在图 11.10 中 IPS 设备对恶意网络行为进行分析。防火墙设备则为内外网之间的安全保护屏障。

试题 3 (2016 年下半年下午试题二)

【说明】

图 11.11 是某互联网企业网络拓扑，该网络采用二层结构，网络安全设备有防火墙、入侵检测系统，楼层接入交换机 32 台，全网划分 17 个 VLAN，对外提供 Web 和邮件服务。

数据库服务器和邮件服务器均安装 CentOS 操作系统(Linux 平台)，Web 服务器安装 Windows 2008 操作系统。

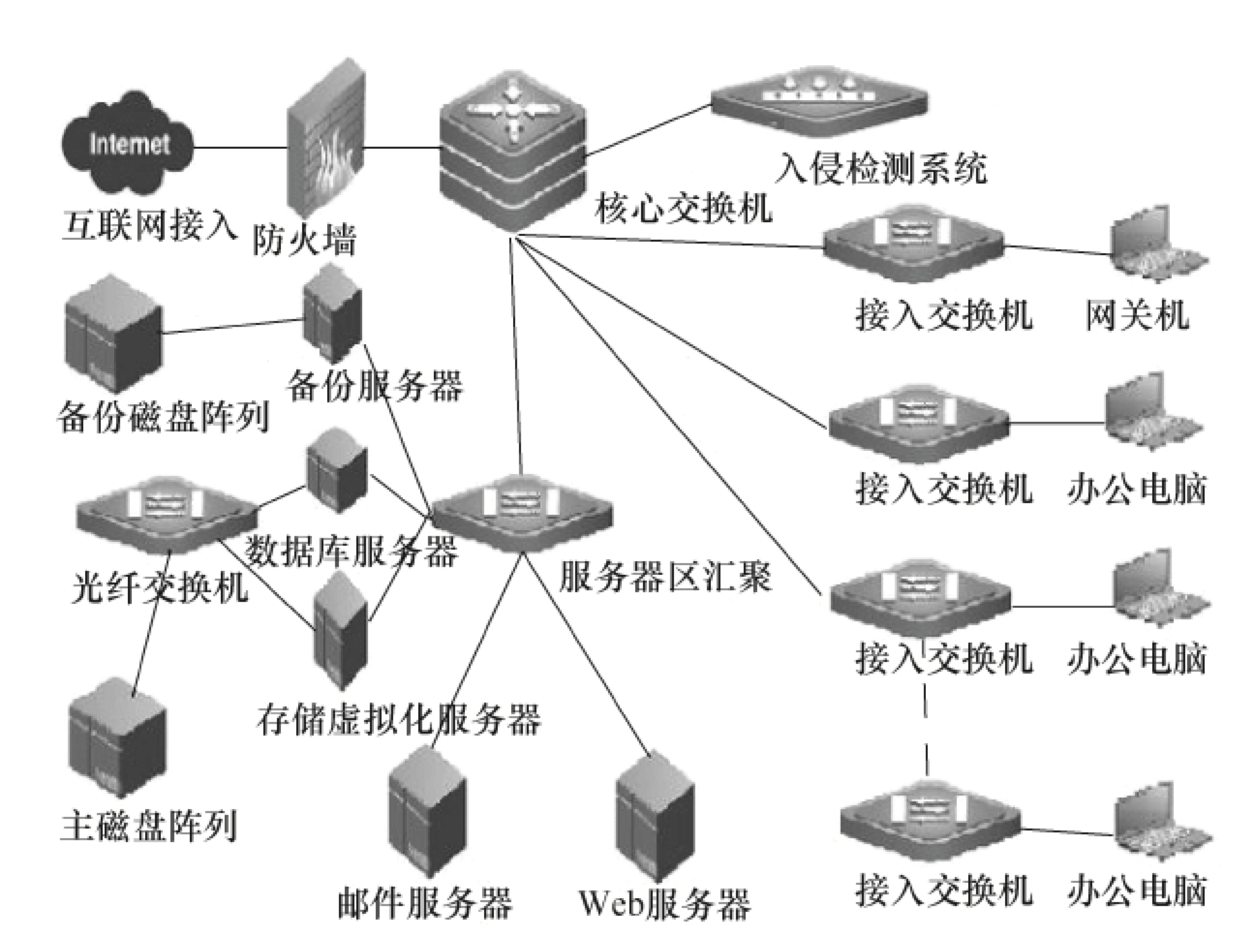


图 11.11 某互联网企业网络拓扑

【问题 1】(6 分)

SAN 常见方式有 FC-SAN 和 IP-SAN，在图 11.11 中，数据库服务器和存储设备连接方式为__(1)__，邮件服务器和存储设备连接方式为__(2)__。虚拟化存储常用文件系统格式有 CIFS、NFS，为邮件服务器分配存储空间时应采用的文件系统格式是__(3)__，为 Web 服务器分配存储空间时应采用的文件系统格式是__(4)__。

【问题 2】(3 分)

该企业采用 RAID5 方式进行数据冗余备份，请从存储效率和存储速率两个方面比较 RAID 1 和 RAID5 两种存储方式，并简要说明采用 RAID5 存储方式的原因。

【问题 3】 (8 分)

网络管理员接到用户反映，邮件登录非常缓慢，按以下步骤进行故障诊断。

1. 通过网管机，利用__(5)__登录到邮件服务器，发现邮件服务正常，但是连接时断时续。

2. 使用__(6)__ 命令诊断邮件服务器的网络连接情况，发现网络丢包严重，登录服务器区汇聚交换机 SI，发现连接邮件服务器的端口数据流量异常，收发包很大。

3. 根据以上情况，邮件服务器的可能故障为__(7)__，应采用__(8)__的办法处理上述故障。

(5)～(8)备选答案：

(5) A. ping　B. ssh　C. tracert　D. mstsc

(6) A. ping　B. telnet　C. tracert　D. netstat

(7) A. 磁盘故障　B. 感染病毒　C. 网卡故障　D. 负荷过大

(8) A. 更换磁盘　B. 安装防病毒软件，并查杀病毒

C. 更换网卡　D. 提升服务器处理能力

【问题 4】(3 分)

上述企业网络拓扑存在的网络安全隐患有：__(9)__、__(10)__、__(11)__。

(9)～(11)备选答案：

A. 缺少针对来自局域网内部的安全防护措施



B. 缺少应用负载均衡
C. 缺少流量控制措施
D. 缺少防病毒措施
E. 缺少 Web 安全防护措施
F. 核心交换机到服务器区汇聚交换缺少链路冗余措施
G. VLAN 划分太多

参考答案：

【问题 1】(1)FC-SAN；(2)IP-SAN；(3)NFS；(4)CIFS。

【问题 2】①存储效率上，RAID5 的存储利用率为$(n-1)/n$，RAID1 的存储利用率为 50%，RAID5 存储效率高。

②存储速率上，RAID5 的速率快于 RAID1。

原因：RAID5 具有数据安全，读写速度快，空间利用率高、成本低的特点。

【问题 3】(5)B；(6)A；(7)B；(8)B。

【问题 4】(9)A；(10)D；(11)E。

要点解析：

【问题 1】

1. SAN 主要包含 FC-SAN 和 IP-SAN 两种。

(1)　存储区域网络(Storage Area Network，SAN)，存储设备组成单独的网络，大多利用光纤连接，采用光纤通道协议(Fiber Channel，FC)。服务器和存储设备间可以任意连接，I/O 请求也是直接发送到存储设备。光纤通道协议实际上解决了底层的传输协议，高层的协议仍然采用 SCSI 协议，所以光纤通道协议实际上可以看成是 SCSI over FC。

(2)　IP-SAN：由于 FC-SAN 的高成本使得很多中小规模存储网络不能接受，一些人开始考虑构建基于以太网技术的存储网络。但是在 SAN 中，传输的指令是 SCSI 的读写指令，不是 IP 数据包。iSCSI(互联网小型计算机系统接口)是一种在 TCP/IP 上进行数据块传输的标准。它是由 Cisco 和 IBM 两家公司发起的，并且得到了各大存储厂商的大力支持。iSCSI 可以实现在 IP 网络上运行 SCSI 协议，使其能够在诸如高速千兆以太网上进行快速的数据存取备份操作。为了与之前基于光纤技术的 FC-SAN 区分开来，这种技术被称为 IP-SAN。iSCSI 继承了两大最传统技术：SCSI 和 TCP/IP 协议。这为 iSCSI 的发展奠定了坚实的基础。

2. CIFS 和 NFS

(1)　CIFS(Common Internet File System)是由 Microsoft 在 SMB 协议的基础上发展，扩展到 Internet 上的协议。它和具体的 OS 无关，在 UNIX 上安装 Samba 后可使用 CIFS。

(2)　NFS(Network File System)即网络文件系统，由 Sun 公司开发，主要用于 UNIX 和类 UNIX 系统，在 Windows 上使用则需要安装客户端软件进行认证时的指令映射。

将 NFS 置于 Windows 上，有两种选择：Microsoft Services for UNIX (SFU)和 DiskShare。CIFS 采用 C/S 模式，基本网络协议：TCP/IP 和 IPX/SPX。

【问题 2】

RAID1 阵列由磁盘对组成，因为需要用做备份，在数据的安全性方面是最好的，但是只能利用磁盘总容量的一半，存储效率只有 50%，存储性能不高。RAID5 是一种存储性能、数据安全和存储成本兼顾的存储解决方案，以 n 块硬盘构建的 RAID5 阵列可以有 $n-1$ 块硬

盘的容量，磁盘空间利用率能达到$(n-1)/n$。在RAID5上，读/写指针可同时对阵列设备进行操作，提供了更高的存储性能。

【问题3】

1. 远程登录到服务器做诊断或配置可以通过Telnet、SSH、远程桌面等方式。

Telnet是C/S构架的服务，登录后是命令行界面，客户端和服务器间的传输无私密性保护，一般用于管理网络设备(如路由器交换机)、Linux或UNIX服务器主机。

SSH和Telnet类似，但是提供私密性保护。

远程桌面管理，是登录上服务器的图形化界面配置，一般用于登录到Windows服务器主机，也可以用于登录到Linux的图形化界面配置，但是需要Linux安装桌面组件。

2. 使用命令诊断邮件服务器的网络连接情况，发现网络丢包严重，根据“丢包”的文字描述，应该是ping命令。

3. 交换机上某个端口数据流量异常，收发包量很大，可能的原因很多，比如病毒、端口或网卡物理故障(不是彻底损坏)、环路导致广播风暴等，但是只有木马类病毒才会故意隐藏自己而让服务正常，只是可能木马窃取数据占用了大量带宽导致一些异常。而其他故障都会导致服务不正常，所以依据本题文字描述，登录上服务器成功，服务正常，综合考虑，病毒的可能性最大。

【问题4】

本题说的是“网络安全隐患”，关于网络的安全隐患和性能以及可用性一定要区别清楚，负载均衡、流量控制、划分VLAN都是性能方面的问题，链路冗余是可用性方面的问题，而防病毒、针对Web的安全防护措施才是安全方面的问题，故B、C、F、G体现的是关于网络可靠性、可用性的特征。

试题4 (2015年下半年下午试题一)

【说明】

某工业园区视频监控网络拓扑如图11.12所示。

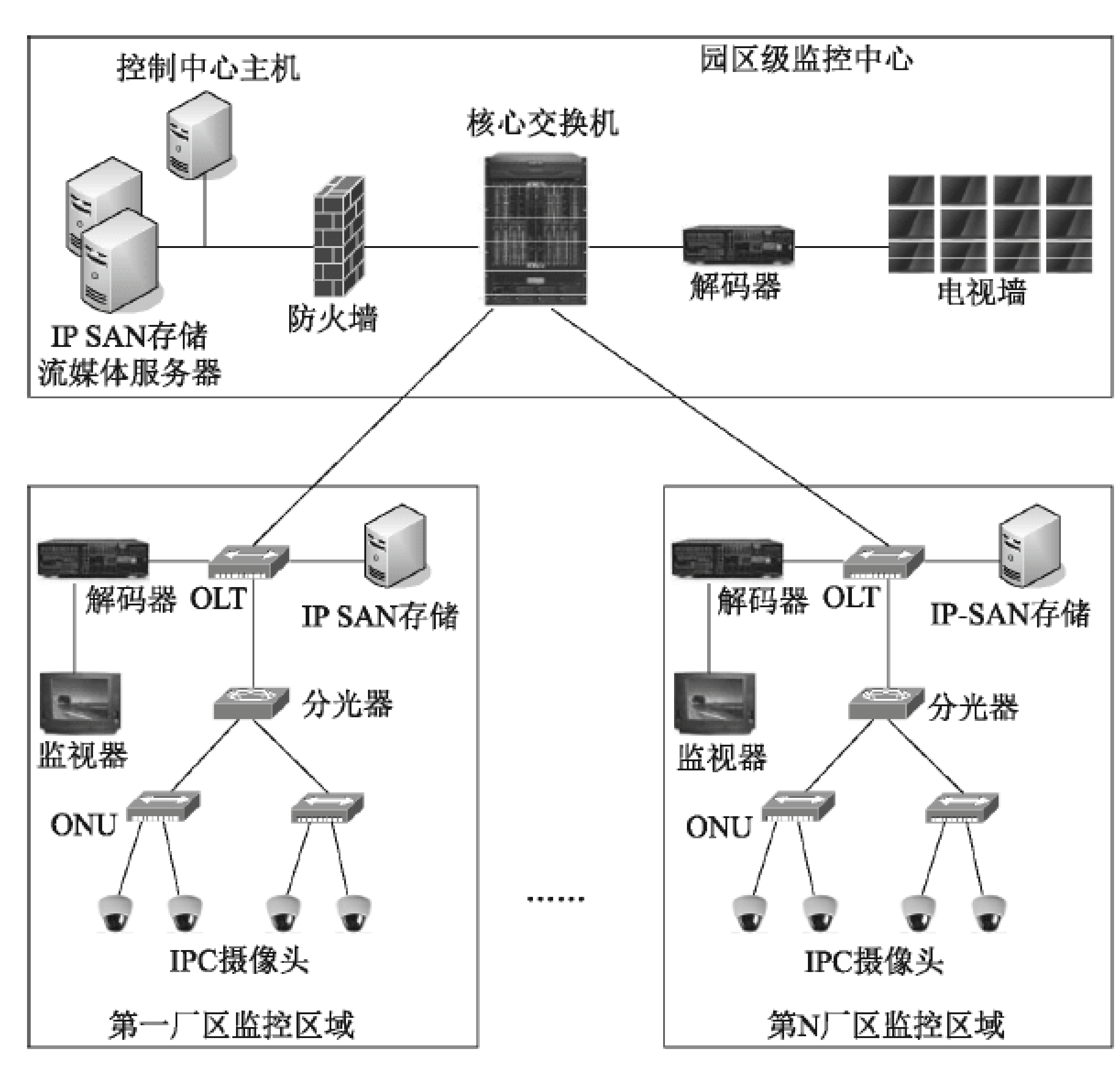


图11.12 某工业园区网络拓扑结构

【问题 1】(4 分)

图 11.12 中使用了 SAN 存储系统，SAN 是一种连接存储管理子系统和 (1) 的专用网络。SAN 分为 FC-SAN 和 IP-SAN，其中 FC-SAN 采用 (2) 互连；IP-SAN 采用 (3) 互连；SAN 可以被看作是数据传输的后端网络，而前端网络则负责正常的 (4) 传输。

(1)～(4)备选答案：

A. iSCSI　　B. TCP/IP　　C. 以太网技术　　D. SATA
E. 文件服务器　　F. 光纤通道技术　　G. 视频管理子系统
H. 存储设备

【问题 2】(4 分)

该网络拓扑是基于 EPON 的技术组网，与传统的基于光纤收发器的组网有所不同。请从组网结构复杂度、设备占用空间大小、设备投资多少、网络管理维护难易程度等几方面对两种网络进行比较。

【问题 3】(6 分)

1. 该系统采用 VLAN 来隔离各工厂和监控点，在 (5) 端进行 VLAN 配置，在 (6) 端采用 trunk 进行 VLAN 汇聚，使用 Manage VLAN 统一管理 OLT 设备。

2. OLT 的 IP 地址主要用于设备的网元管理，一般采用 (7) 方式分配，IPC 摄像机的地址需要统一规划，各厂区划分为不同的地址段。

【问题 4】(6 分)

1. 在视频监控网络中，当多个监控中心同时查看一个点的视频时要求网络支持 (8) 。

(8)备选答案：

A. IP 广播　　B. IP 组播　　C. IP 任意播

2. 在组网时，ONU 设备的 (9) 接口通过 UTP 网线和 IPC 摄像机连接。

(9)备选答案：

A. BNC　　B. RJ-45　　C. USB

3. 该网络的网管解决方案中一般不包含 (10) 功能或组件。

(10)备选答案：

A. 网元管理　　B. 防病毒模块
C. EPON 系统管理　　D. 事件、告警管理

参考答案：

【问题 1】

(1)G；(2)F；(3)A；(4)B。

【问题 2】

对比内容	光纤收发器	EPON
组网结构	复杂	简单
占用空间	较多	较少
设备投资	较多	较少
管理维护	复杂	简单

【问题 3】

(5)ONU；(6)OLT；(7)手动或静态。

【问题 4】

(8)B；(9)B；(10)B。

要点解析：

【问题 1】

SAN 是一种连接存储管理子系统和视频管理子系统的专用网络。在视频处理领域里，SAN 就像数字视频网络中的大本营，不但承担着视频数据的存储、迁移、交换、共享，而且掌管着网络设备的登记、删除、查询、维护。可以这么理解，SAN 是电视台视频网络的主干，在 SAN 网上可以挂接诸如新闻生产系统、非线性编辑系统、广告非线性插播系统、数字化节目库系统等。

FC-SAN(存储区域网络)和 NAS 不同，它不是把所有的存储设备集中安装在一个专门的 NAS 服务器中，而是通过光纤交换设备将磁盘阵列、磁带等存储设备与相关服务器连接起来组成一个高速专用子网，然后与企业现有的局域网进行连接。SAN 可以被看作是负责存储传输的后端网络，而前端的数据网络负责正常的 TCP/IP 传输。

如果 SAN 是基于 TCP/IP 的网络，使用 IP-SAN 网络。这种方式是将服务器和存储设备通过 iSCSI 技术连接起来，就是把 SCSI 命令包在 TCP/IP 包中传输，即为 SCSI over TCP/IP。

【问题 2】

EPON 是基于以太网的无源光网络，无源设备可靠性高。比传统的基于光纤收发器的组网结构简单、设备占用空间小、设备投资少、网络管理难度低等。

组网结构复杂度：EPON 采用点到多点结构，无源光纤传输，结构简单。

设备占空间大小：EPON 由局端 OLT、用户端 ONU、光分配网 ODN 组成，设备占用空间小。

设备投资方面：EPON 采用的 OLT、ONU、ODN 光网设备，无须租用机房，无须配备电源，因此成本投资少。

网络维护管理：EPON 由于不用配备有源维护人员，采用 OLT 技术统一管理，维护容易。

【问题 3】

1. 该系统采用 VLAN 来隔离各工厂和监控点，在 ONU 端进行 VLAN 配置，在 OLT 端采用 trunk 进行 VLAN 汇聚，使用 Manage VLAN 统一管理 OLT 设备。

2. OLT 的 IP 地址主要用于设备的网元管理，一般采用手动或静态方式分配，IPC 摄像机的地址需要统一规划，各厂区划分为不同的地址段。

【问题 4】

TCP/IP 传输方式有 3 种：单播、广播、组播。单播在发送和每个接收主机之间需要单独的数据信道，如果有多个主机希望获得数据包的同一份拷贝将导致发送端负担沉重、延迟长、网络拥塞。组播是允许一个或多个主机发送一个数据包到多个主机的网络技术。组播源把数据包发送到特定组播组，只有属于该组播组地址的主机才能接收到数据包。广播是指在 IP 子网内广播数据包，所有在子网内部的主机都将收到这些数据包。

UTP 网线由一定长度的双绞线和 RJ-45 水晶头组成。双绞线由 8 根不同颜色的线分成 4 对绞合在一起，成对扭绞的作用是尽可能减少电磁辐射与外部电磁干扰的影响。

防病毒模块属于网络安全防护的范畴，随着网络病毒特征的变化需要不断地升级病毒库。该模块与具体的网络设备的配置管理、运行维护和故障监控之间密切度不高， 一般不作为特定网络管理解决方案的组成部分。

试题 5 （2015 年上半年下午试题一）

【说明】

某企业网络拓扑图如图 11.13 所示。

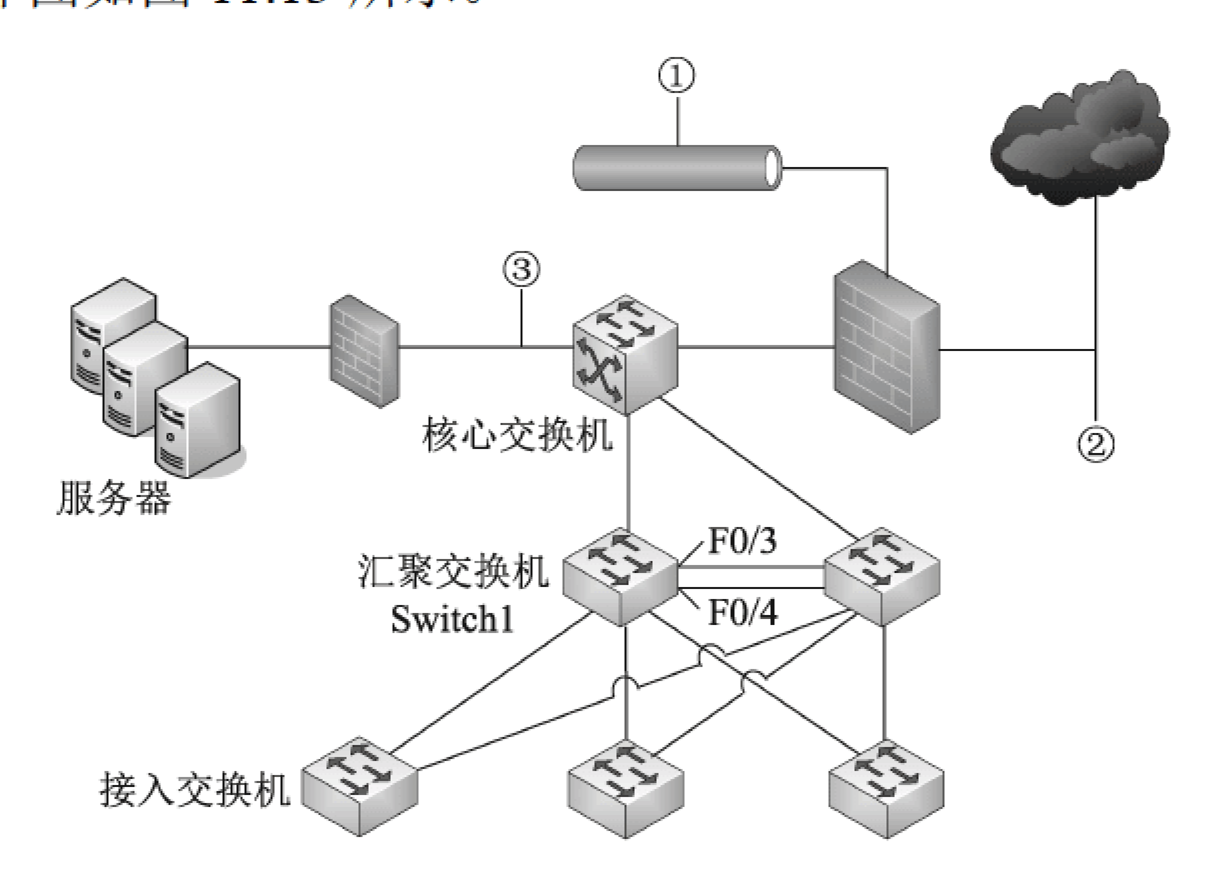


图 11.13　某企业网络拓扑图

工程师给出了该网络的需求：

1. 用防火墙实现内外网地址转换和访问控制策略；
2. 核心交换机承担数据转发，并且与汇聚层两台交换机实现 OSPF 功能；
3. 接入层到汇聚层采用双链路方式组网；
4. 接入层交换机对地址进行 VLAN 划分；
5. 对企业的核心资源加强安全防护。

【问题 1】(4 分)

该企业计划在①、②或③的位置部署基于网络的入侵检测系统(NIDS)，将 NIDS 部署在①的优势是__(1)__；将 NIDS 部署在②的优势是__(2)__、__(3)__；将 NIDS 部署在③的优势是__(4)__。

(1)～(4)备选答案：

A. 检测外部网络攻击的数据和类型

B. 监视针对 DMZ 中系统的攻击

C. 监视针对关键系统、服务和资源的攻击

D. 能减轻拒绝服务攻击的影响

【问题 2】(4 分)

OSPF 主要用于大型、异构的 IP 网络中，是对__(5)__路由的一种实现。若网络规模较小，可以考虑配置静态路由或__(6)__协议实现路由选择。

(5)备选答案：A. 链路状态　　　　B. 距离矢量　　　　C. 路径矢量

(6)备选答案：A. EGP　　B. RIP　　C. BGP

【问题3】(4分)

对汇聚层两台交换机的F0/3、F0/4端口进行端口聚合，F0/3、F0/4端口默认模式是__(7)__，进行端口聚合时应配置为__(8)__模式。

(7)、(8)备选答案：

A. multi　　B. trunk　　C. access

【问题4】(6分)

为了在汇聚层交换机上实现虚拟路由冗余功能，需配置__(9)__协议，可以采用竞争的方式选择主路由设备，比较设备优先级大小，优先级大的为主路由设备。若备份路由设备长时间没有收到主路由设备发送的组播报文，则将自己的状态转为__(10)__。

为了避免二层广播风暴，需要在接入与汇聚设备上配置__(11)__。

(10)、(11)备选答案：

A. Master　　B. Backup　　C. VTP Server　　D. MSTP

【问题5】(2分)

阅读汇聚交换机Switch 1的部分配置命令，回答下面的问题。

```
Switch 1(config)#interface vlan 20
Switch 1 (config-if)#ip address 192.168.20.253 255.255.255.0
Switch 1(config-if)#standby 2 ip 192.168.20.250
Switch 1(config-if)#standby 2 preempt
Switch 1(config-if)#exit
```

VLAN20standby默认优先级的值是__(12)__。

VLAN20设置preempt的含义是__(13)__。

参考答案：

【问题1】

(1)B；(2)A；(3)D；(4)C。

【问题2】

(5)A；(6)B。

【问题3】

(7)C；(8)B。

【问题4】

(9)HSRP；(10)A；(11)D。

【问题5】

(12)100；(13)设置抢占模式。

要点解析

【问题1】

由图中可知，①位于DMZ区，所以可以监视针对DMZ中系统的攻击。②连接外网，所以可以检测外部网络攻击的数据和类型、减轻拒绝服务攻击的影响。③位于内网服务器区域，所以可以监视针对关键系统、服务和资源的攻击。



【问题 2】

OSPF 属于链路状态路由协议。网络规模小，可采用 RIP 路由协议，而 EGP 和 BGP 属于外部网关路由协议。

【问题 3】

交换机默认端口的模式为接入模式 access，对汇聚层交换机进行端口聚合时，一般配置为 trunk 模式。

【问题 4】

汇聚交换机采用虚拟路由冗余，目的是当一台汇聚交换机出现故障时，启用备份线路的措施。根据设备情况可以采用虚拟路由器冗余协议(VRRP)或热备份路由器协议 (HSRP)。生成树协议是一种二层管理协议，它通过有选择性地阻塞网络冗余链路来达到消除网络二层环路的目的，同时具备链路的备份功能。

【问题 5】

```
Switch1(config)#interface vlan 20  //进入 VLAN20 虚接口
Switch1(config-if)#ip address 192.168.20.253 255.255.255.0 //配置 IP 地址
Switch1(config-if)#standby 2 ip 192.168.20.250  //配置备份组 2 的虚拟 IP
Switch1(config-if)#standby 2 preempt   //配置抢占功能
Switch1(config-if)#exit
```

默认优先级为 100，取值范围为 0～255，值越大，优先级越高。

11.4　强化训练

11.4.1　综合知识试题

试题 1　(2014 年下半年试题 34)

搭建试验平台、进行网络仿真是网络生命周期中__(34)__阶段的任务。

(34) A. 需求规范　　B. 逻辑网络设计
C. 物理网络设计　　D. 实施

试题 2　(2014 年下半年试题 67 和试题 68)

结构化布线系统分为六个子系统，其中水平子系统的作用是__(67)__，园区子系统的作用是__(68)__。

(67)、(68) A. 连接各个建筑物中的通信系统
B. 连接干线子系统和用户工作区
C. 实现中央主配线架与各种不同设备之间的连接
D. 实现各楼层设备间子系统之间的互连

试题 3　(2014 年下半年试题 69)

网络系统设计过程中，逻辑网络设计阶段的任务是__(69)__。

(69) A. 对现有网络资源进行分析，确定网络的逻辑结构

B. 根据需求说明书确定网络的安全系统架构
C. 根据需求规范和通信规范，分析各个网段的通信流量
D. 根据用户的需求，选择特定的网络技术、网络互连设备和拓扑结构

试题 4 (2014 年下半年试题 70)

下列关于网络汇聚层的描述中，正确的是__(70)__。

(70) A. 要负责收集用户信息，例如用户 IP 地址、访问日志等
B. 实现资源访问控制和流量控制等功能
C. 将分组从一个区域高速地转发到另一个区域
D. 提供一部分管理功能，例如认证和计费管理等

试题 5 (2014 年上半年试题 33)

结构化综合布线系统中的干线子系统是指__(33)__。

(33) A. 管理楼层内各种设备的子系统　　B. 连接各个建筑物的子系统
C. 工作区信息插座之间的线缆子系统　　D. 实现楼层设备间连接的子系统

试题 6 (2014 年上半年试题 70)

网络系统设计过程中，物理网络设计阶段的任务是__(70)__。

(70) A. 依据逻辑网络设计的要求，确定设备的具体物理分布和运行环境
B. 分析现有网络和新网络的各类资源分布，掌握网络所处的状态
C. 根据需求规范和通信规范，实施资源分配和网络规划
D. 理解网络应该具有的功能和性能，最终设计出符合用户需求的网络

11.4.2 案例分析试题

试题 1 (2014 年下半年下午试题一)

【说明】

某企业的网络结构如图 11.14 所示。

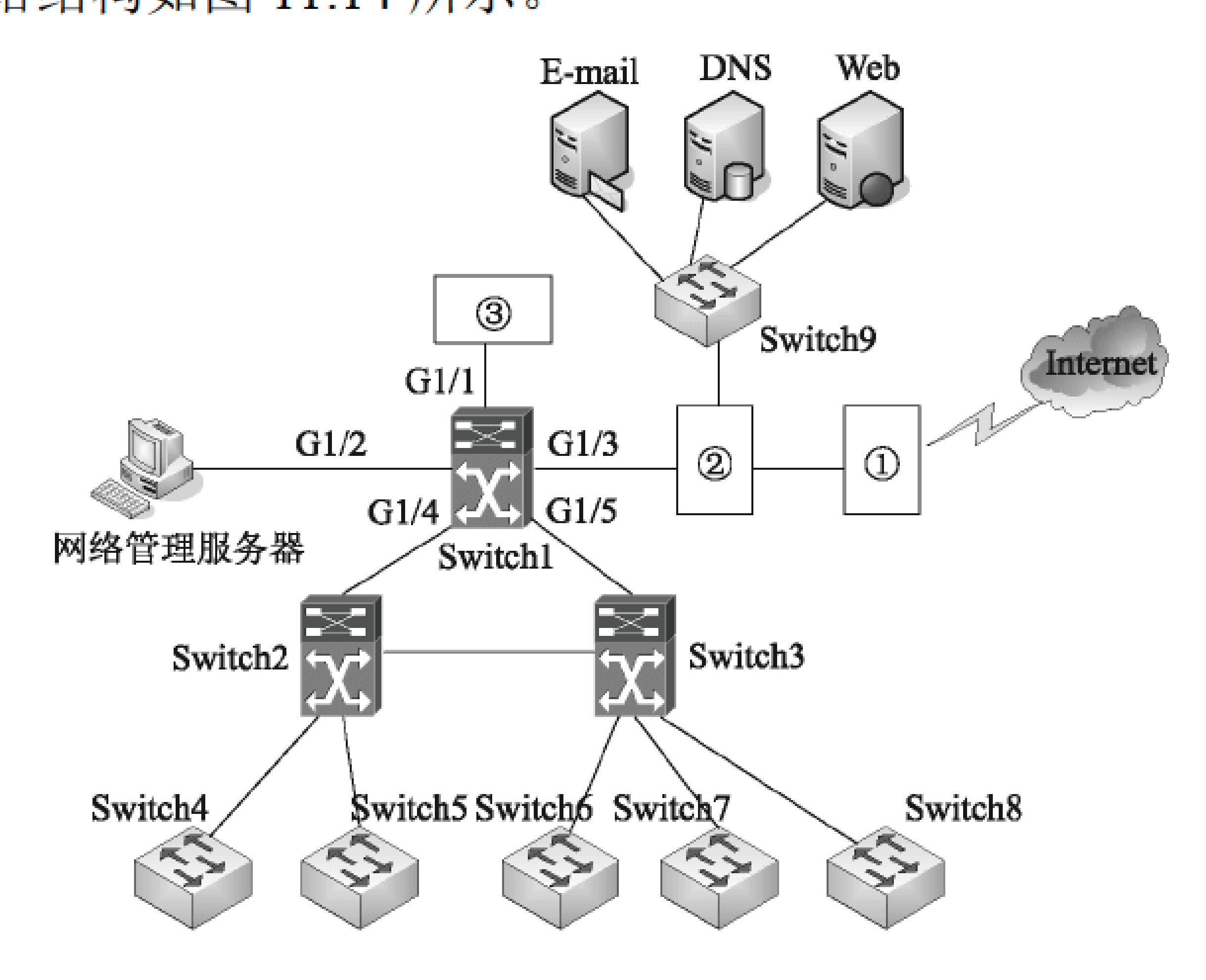


图 11.14 某企业的网络结构



【问题 1】(6 分)

1. 图 11.14 中的网络设备①应为__(1)__，网络设备②应为__(2)__，从网络安全的角度出发，Switch9 所组成的网络一般称为__(3)__区。

2. 图 11.14 中③处的网络设备的作用是检测流经内网的信息，提供对网络系统的安全保护。该设备提供主动防护，能预先对入侵活动和攻击性网络流量进行拦截，避免造成损失，而不是简单地在恶意流量传送时或传送后才发出警报。网络设备③应为__(4)__，其连接的 Switch1 的 G1/1 端口称为__(5)__端口，这种连接方式一般称为__(6)__。

【问题 2】(5 分)

1. 随着企业用户的增加，要求部署上网行为管理设备，对用户的上网行为进行安全分析、流量管理、网络访问控制等，以保证正常的上网需求。部署上网行为管理设备的位置应该在图 11.14 中的__(7)__和__(8)__之间比较合理。

2. 网卡的工作模式有直接、广播、多播和混杂四种模式，缺省的工作模式为__(9)__和__(10)__，即它只接收广播帧和发给自己的帧。网络管理机在抓包时，需要把网卡置于__(11)__模式，这时网卡将接受同一子网内所有站点所发送的数据包，这样就可以达到对网络信息监视的目的。

【问题 3】(5 分)

针对图 11.14 中的网络结构，各台交换机需要运行__(12)__协议，以建立一个无环路的树状网络结构。按照该协议，交换机的默认优先级值为__(13)__，根交换机是根据__(14)__来选择的，值小的交换机为根交换机；如果交换机的优先级相同，再比较__(15)__。当图 11.14 中的 Switch1—Switch3 之间的某条链路出现故障时，为了使阻塞端口直接进入转发状态，从而切换到备份链路上，需要在 Switch1—Switch3 上使用__(16)__功能。

【问题 4】(4 分)

根据层次化网络的设计原则，从图 11.14 中可以看出该企业网络采用了由__(17)__层和__(18)__层组成的两层架构，其中，MAC 地址过滤和 IP 地址绑定等功能是由__(19)__完成的，分组的高速转发是由__(20)__完成的。

试题 2 (2014 年上半年下午试题一)

【说明】

某单位计划部署园区网络，该单位总部设在 A 区，另有两个分别设在 B 区和 C 区，各个地区之间距离分布如图 11.15 所示。

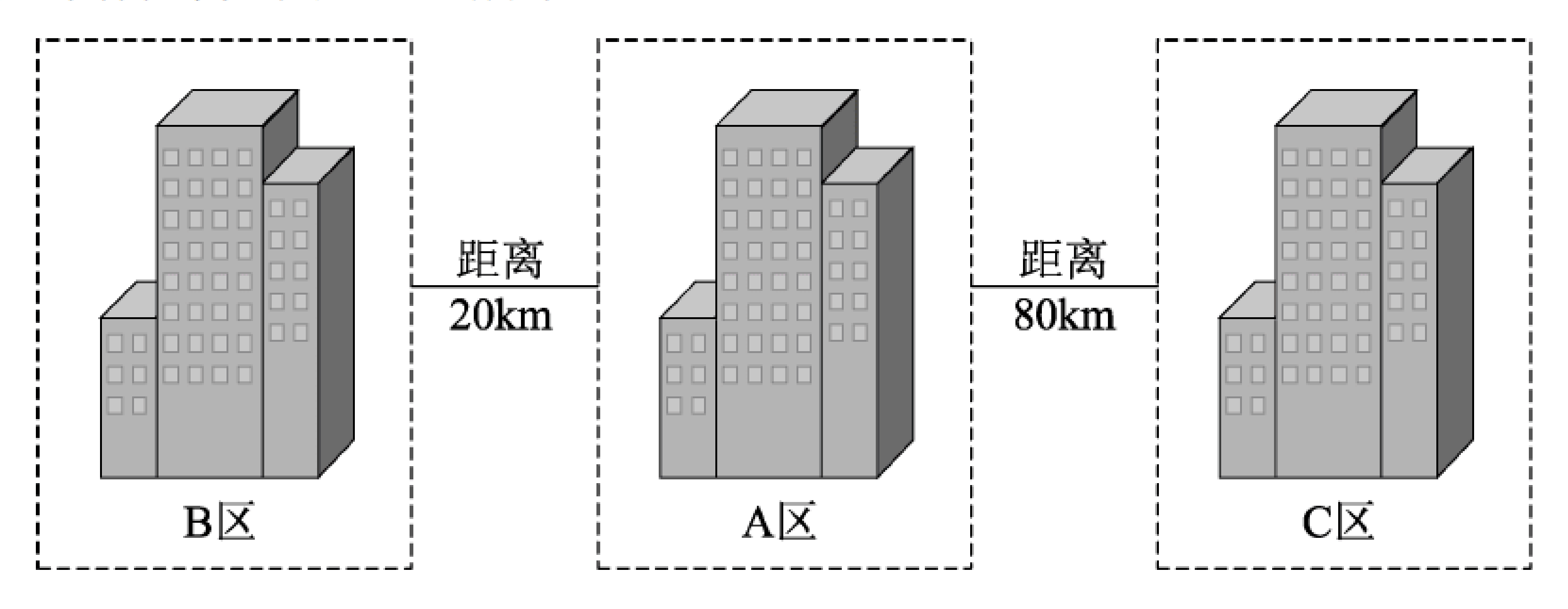


图 11.15　各地区之间距离分布

该单位的主要网络业务需求在A区，该网络中心及服务器机房亦部署在A区；B区的网络业务流量需求远大于C区；C区虽然业务流量小，但是网络可靠性要求高。根据业务需要，要求三个区的网络能够互通并且都能够访问互联网，同时基于安全考虑单位要求采用一套认证设备进行身份认证和上网行为管理。

【问题1】(6分)

为了保障业务需求，该单位采用两家运营商接入Internet。根据题目需求，回答下列问题。

1. 两家运营商的Internet 接入线路应部署在哪个区？为什么？
2. 网络运营商提供的MPLS-VPN和千兆裸光纤两种互连方式，哪一种可靠性高？为什么？
3. 综合考虑网络需求及运营成本，在AB区之间与AC区之间分别采用上述哪种方式进行互连？

【问题2】(8分)

该单位网络部署接入点情况如表11.3所示。

表11.3　单位网络部署接入点情况

区　域	汇 聚 点	接 入 点	备　注
A	办公楼	124	所有区域采用三层局域网结构部署，其中A区采用双核心交换机冗余。所有汇聚点采用单模光纤上联至核心交换机。所有接入交换机采用双绞线上联至汇聚交换机
	资料室	86	
	网管中心	78	
	设计中心	200	
	生产区	115	
B	办公楼	106	
	培训中心	126	
	宿舍	198	
C	办公楼	86	
	营销中心	54	

根据网络部署需求，该单位采购了相应的网络设备，请根据题目说明及表11.3，确定表11.4所示的设备数量及合理的部署位置(注：不考虑双绞线的距离限制)。

表11.4　设备及部署区域

设备类型	设备数量	部署区域
核心交换机	__(1)__	A区
核心交换机	1	B区
核心交换机	1	C区
汇聚交换机	5	A区
汇聚交换机	3	B区
汇聚交换机	2	C区
SFP单模模块	5	__(2)__区
SFP单模模块	7	__(3)__区

续表

设备类型	设备数量	部署区域
SFP 单模模块	22	__(4)__ 区
24 口接入交换机	__(5)__	A 区
24 口接入交换机	__(6)__	B 区
24 口接入交换机	__(7)__	C 区
千兆服务器接入交换机	1	A 区
服务器	3	A 区
服务器	1	__(8)__ 区
认证及流控设备	1	A 区
防火墙	1	A 区

【问题 3】(6 分)

根据题目要求，在图 11.16 的方框中画出该单位 A 区网络拓扑示意图(汇聚层以下不画)。

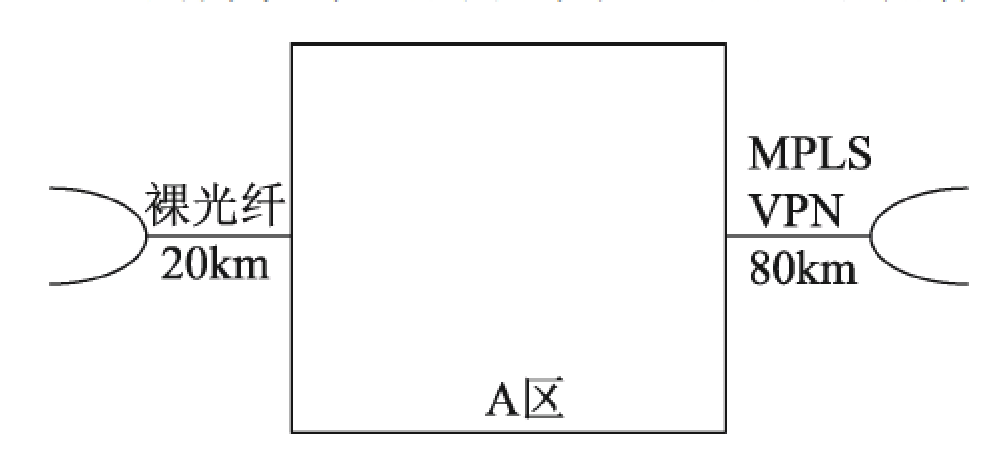


图 11.16　问题 3 图示

11.4.3　综合知识试题参考答案

【试题 1】答　案：(34)B。

解　析：五阶段周期是一种较为常见的迭代周期划分方法，它将一次迭代划分成 5 个阶段：需求规范、通信规范、逻辑网络设计、物理网络设计、实施阶段。

逻辑网络设计根据需求规范和通信规范选择一种比较适宜的网络逻辑结构，并实施后续的资源分配规划、安全规划等内容。网络逻辑结构要根据用户需求中描述的网络功能、性能等要求来进行设计，而且要根据网络用户的分类和分布，形成特定的网络结构。在逻辑网络设计阶段，通过搭建试验平台、进行网络仿真，以确定合理的网络结构，选用成熟而稳定的技术等。

【试题 2】答　案：(67)B；(68)A。

解　析：结构化布线系统分为 6 个子系统：工作区子系统、水平子系统、干线子系统、设备间子系统、管理子系统和建筑群子系统。

水平子系统是结构化综合布线系统中连接用户工作区与布线系统主干的子系统。水平子系统由每层配线间至信息插座的配线电缆和工作区用的信息插座等组成。在结构化综合布线系统中，水平子系统起着支线的作用，它将所有用户端通过一些连接件连接到配线设备上。

园区子系统也称为建筑群子系统，是结构化综合布线系统中由连接楼群之间的通信传输介质及各种支持设备组成的子系统。

【试题3】答　案：(69)D。

解　析：逻辑网络设计根据需求规范和通信规范选择一种比较适宜的网络逻辑结构，并实施后续的资源分配规划、安全规划等内容。网络逻辑结构要根据用户需求中描述的网络功能、性能等要求来进行设计，而且要根据网络用户的分类和分布，形成特定的网络结构。

【试题4】答　案：(70)B。

解　析：大型局域网可以划分为多个层次，层次化模型中最典型的是三层模型，这种模型允许在三个路由或交换层次上实现流量汇聚和分组过滤功能。三层模型将网络划分为核心层、汇聚层和接入层，每一层都有着特定的作用。核心层提供不同区域之间的最佳路由和高速数据传送；汇聚层将网络业务连接到接入层，并且实施与安全、流量、负载和路由相关的策略；接入层为用户提供了在本地网段访问应用系统的能力，还要解决相邻用户之间的互访需要，接入层要负责一些用户信息(例如用户IP地址、MAC地址和访问日志等)的收集工作和用户管理功能(包括认证和计费等)。

【试题5】答　案：(33)D。

解　析：整个综合布线系统通常由工作区子系统、水平子系统、干线子系统、设备间子系统、管理子系统和建筑群主干子系统6个部分组成。

(1) 工作区子系统：是用户终端设备的子系统，主要包括信息插座、信息插座和设备之间的适配器。通俗地说，就是指电脑和网线接口之间的部分。

(2) 水平子系统：是连接工作区与主干的子系统，主要包括配线架、配线电缆和信息插座。通俗地说，就是指从楼层弱电井里的配线架到每个房间的网卡接口之间的部分。通常布线是在天花板上，因此与楼层平行。在水平子系统中，使用的是星型拓扑结构，即将每个网卡接口(信息模块)接回配线架，每个口一根线。

(3) 管理子系统：管理子系统是对布线电缆进行端接及配置管理的子系统，通常在各个楼层都会设立。通俗地讲，这就是配线间中的设备部分。

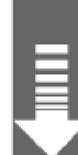
(4) 干线子系统：是用来连接管理间、设备间的子系统。通俗地说，就是将接入层交换机连接到分布层(或核心层)交换机的网络线路。由于其通常是顺着大楼的弱电井而下，与大楼垂直，因此也称为垂直子系统。通常来说，干线经常使用光缆，另外高品质的5类/超5类以及6类非屏蔽双绞线也是十分常用的。

(5) 设备间子系统：是安装在设备间的子系统，而设备间是指集中安装大型设备的场所。一般来说，大型建筑物都会有一个或多个设备间。通常核心交换机所在的位置就是设备间。它与管理子系统相比，对物理环境的要求更高。

(6) 建筑群主干子系统：它是用来连接楼群之间的子系统，包括各种通信传输介质和支持设备，由于在户外，因此又称为户外子系统。它通常包括地下管道、直埋沟内、架空三种方式。现在许多新的建筑物，通常都会预先留好地下管道。

【试题6】答　案：(70)A。

解　析：物理网络设计包含物理设备选型、网络中心机房设计、综合布线系统设计、物理网络设计文档等内容。B选项是需求分析阶段，C和D选项都是逻辑网络设计的内容。



11.4.4　案例分析试题参考答案

试题 1　答案与解析

答　案：

【问题 1】

(1)路由器；(2)防火墙；(3)DMZ；(4)IPS；(5)镜像；(6)旁路模式。

【问题 2】

(7)防火墙；(8)SW1；(9)直接；(10)广播；(11)混杂。

【问题 3】

(12)STP；(13)32768；(14)交换机 ID；(15)MAC 地址；(16)上行速链路。

【问题 4】

(17)核心层；(18)接入层；(19)接入层；(20)核心层。

解　析：

【问题 1】

网络设备①接入 Internet 应为路由器，那么设备②即为防火墙，Switch9 所接区域应为 DMZ 区。

根据该设备提供主动防护，能预先对入侵活动和攻击性网络流量进行拦截，避免造成损失，而不是简单地在恶意流量传送时或传送后才发出警报，可判断设备③为 IPS，则其连接的 G1/1 端口称为镜像端口，这样的连接方式为旁路模式。一般 IPS 以串接的方式接入网络，但是此题的部署方式并不常规，根据题意预先对入侵活动和攻击性网络流量进行拦截，避免造成损失来判断应为 IPS。

【问题 2】

上网行为管理是指帮助互联网用户控制和管理对互联网的使用，包括对网页访问过滤、网络应用控制、带宽流量管理、信息收发审计、用户行为分析，上网行为管理设备的位置应该在防火墙和 SW1 之间。

网卡具有如下几种工作模式。

(1)　广播模式(Broad Cast Model)：它的物理地址(MAC)地址是 0Xffffff 的帧为广播帧，工作在广播模式的网卡接收广播帧。

(2)　多播传送(MultiCast Model)：多播传送地址作为目的物理地址的帧可以被组内的其他主机同时接收，而组外主机却接收不到。但是，如果将网卡设置为多播传送模式，它可以接收所有的多播传送帧，而不论它是不是组内成员。

(3)　直接模式(Direct Model)：工作在直接模式下的网卡只接收目地址是自己 MAC 地址的帧。

(4)　混杂模式(Promiscuous Model)：工作在混杂模式下的网卡接收所有的流过网卡的帧，信包捕获程序就是在这种模式下运行的。

网卡的缺省工作模式包含广播模式和直接模式，即它只接收广播帧和发给自己的帧。如果采用混杂模式，一个站点的网卡将接受同一网络内所有站点所发送的数据包，这样就可以达到对于网络信息监视捕获的目的。

【问题 3】

生成树算法的网桥协议 STP(Spanning Tree Protocol)通过生成树来保证一个已知的网桥在网络拓扑中沿一个环动态工作。

STP 的算法分为 3 个步骤。

(1) 选择根网桥(Root Bridge)，依据：网桥 ID(BID)= 网桥优先级+网卡的 MAC 地址，其中网桥 ID 是唯一的，以及选择交换网络中网桥 ID 最小的交换机成为根网桥。注意：优先级取值范围为 0～65535，缺省值为 32768。

(2) 选择根端口(Root Ports)，依据：到根网桥最低的根路径成本，直连的网桥 ID 最小，直连的端口 ID 最小。注意：端口 ID=端口优先级+端口编号，端口优先级范围为 0～255，缺省值为 128。其中根路径成本为：网桥到根网桥的路径上所有链路的成本之和。

(3) 选择指定端口(Designated Ports)。

配置上行速链路，当接入层或汇聚层的交换机主用的上行链路断开的时候，被阻塞的端口迅速转换到转发的状态，不需要经历侦听和学习状态。

【问题 4】

层次化网络模型包括：

(1) 由经过可用性和性能优化的高端路由器和交换机组成的核心层。

(2) 由用于实现策略的路由器和交换机构成的汇聚层。

(3) 通过用以连接用户的低端交换机等构成的接入层。

核心层是网络高速交换的主干，接入层为用户提供了在本地网段访问应用系统的能力，具有过滤 MAC 地址、绑定 IP 地址等功能。

试题 2 答案与解析

答　案：

【问题 1】

1. A 区。原因：A 区是网络中心，B 区和 C 区接入 Internet 流量都需要经过 A 区。

2. 裸光纤高。原因：MPLS-VPN 是本地线路走 SDH 专线，链接到运营商的专网 MPLS-VPN。裸光纤是物理层的点对点链接，所以可靠性当然是裸光纤高。

3. AB 区之间用裸光纤，AC 区之间用 MPLS-VPN。

【问题 2】

(1)2；(2)C；(3)B；(4)A；(5)27；(6)19；(7)7；(8)A。

【问题 3】

A 区网络拓扑如图 11.17 所示。

解　析：

【问题 1】

本题考查的是网络规划的基本知识。

本问题考查广域网接入及网络互连的问题。

1. 两家运营商的 Internet 接入线路应部署在 A 区。其主要原因有两点：首先，根据题目描述该单位的主要网络业务需求在 A 区，网络中心及服务器机房亦部署在 A 区，另外，该单位要求采用一套认证设备进行身份认证和上网行为管理，所以出口线路应集中在一个

业务需求大的区域(A 区)。这时，由于三个区域是互通的，其他区域也可通过 A 区出口与互联网连接。

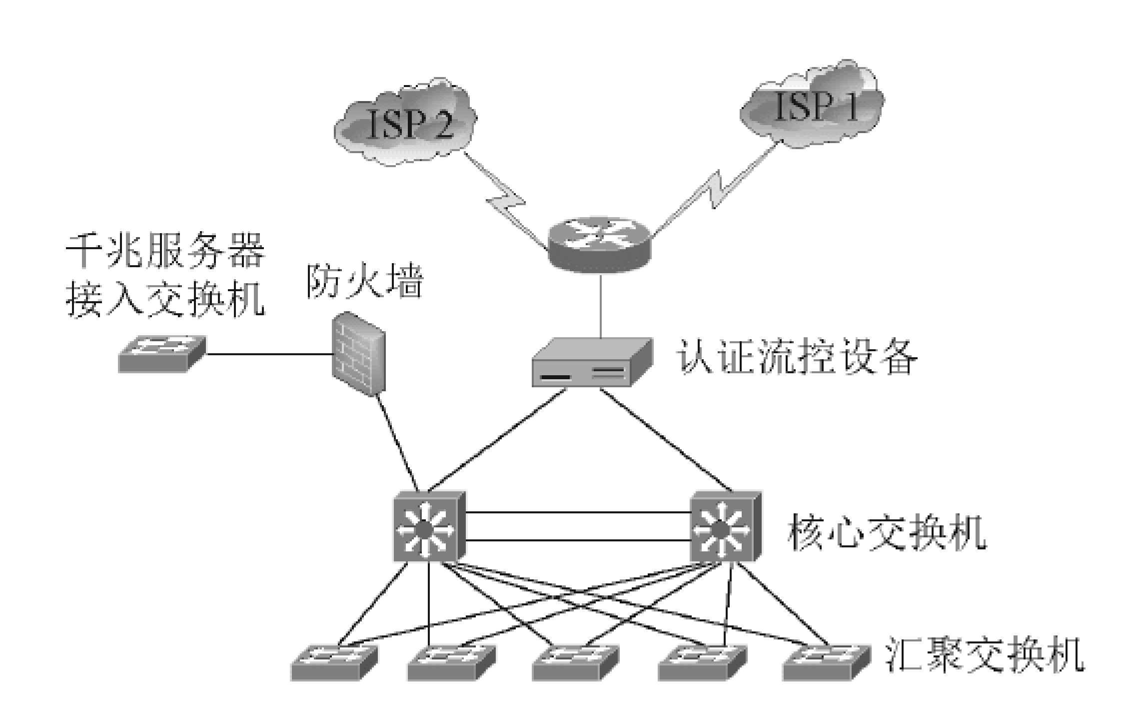


图 11.17　A 区网络拓扑示意图

2. 网络运营商提供了 MPLS VPN 和千兆裸光纤两种互连方式。这两种互连方式中 MPLS VPN 的可靠性大于千兆裸光纤，这是由于当千兆裸光纤是物理链路，当其出现链路故障时，互连业务就会中断。MPL SVPN 属于逻辑链路。当单个物理链路出现故障时，只要其他链路可达，MPLS VPN 还可提供互连服务。

3. 综合考虑网络需求及运行成本，AB 区之间应采取千兆裸光纤互连模式，AC 区之间应采用 MPLS VPN 互连方式。

根据题目描述，B 区的网络业务流量需求远大于 C 区：C 区虽然业务量小，但是网络可靠性要求高。所以，AB 区之间采取千兆裸光纤以适应大业务量，AC 区之间采用 MPLS VPN 在业务量不大但安全性要求较高时是合理的。

【问题 2】

本题考查的是网络设备选型的基础知识。

1. 根据题目描述可知，A 区采用双核心交换机冗余，所以 A 区核心交换机的数量为 2 台。

2. 根据题目描述可知，所有汇聚点采用单模光纤上联至核心交换机 SFP 单模模块。A、B、C 区的汇聚交换机分别有 5、3、2 台，其中 A 区是双核心交换机，故核心与汇聚相连需要 20 个 SFP 单模模块，另外 A 区需要和 B、C 区核心交换机互连，所以还需要 2 个 SFP 单模模块，共计 22 个。同样可以推算出 B 区需要 7 个 SFP 单模模块，C 区需要 5 个 SFP 单模模块。

3. A、B、C 区的接入点数参见表 11.3，不考虑双绞线的距离限制，只需要计算同一个楼内需要的 24 口接入交换机数量即可。根据计算可知，A 区需要 24 口接入交换机 28 个，B 区需要 24 口接入交换机 20 个，C 区需要 24 口接入交换机 7 个。

4. 由前述可知，Internet 接入线路部署在 A 区，所以路由器应部署在 A 区。

【问题 3】

A 区采用双核心交换机，汇聚层可采用单模光纤双线冗余上联至两台核心交换机，核心交换机之间可通过以太网通道技术以提高带宽和链路备份。

核心交换机可直接连入防火墙，防火墙通过千兆服务器接入交换机保障服务器区域的安全。双核心交换机共两条光纤连接认证与流控设备，最后由认证与流控设备连接出口路由器，出口路由器采用双 ISP 互连方式进入 Internet。

第 12 章 计算机基础知识

12.1 备考指南

12.1.1 考纲要求

根据考试大纲中相应的考核要求，在“计算机基础知识”知识模块上，要求考生掌握以下方面的内容。

1. 计算机硬件部分

(1) 计算机组成，包括计算机部件、指令系统、多处理器、多处理器的性能。

(2) 存储器，包括存储介质存储系统、主存与辅存、主存类型、主存容量和性能、主存配置、高速缓存、辅存设备的性能和容量计算。

(3) 输入/输出结构和设备，中断、DMA、通道、SCSI、I/O 接口、输入和输出设备类型和特征。

2. 操作系统部分

(1) 操作系统的基本概念，包括操作系统的定义和特征、功能及分类，以及多道程序、内核和中断控制、进程和线程。

(2) 处理机管理、存储管理、设备管理、文件管理、作业管理，包括进程的状态及转换、进程调度算法、死锁、存储管理方案、文件管理、作业调度算法。

(3) 系统管理，包括系统性能和系统可靠性。

3. 系统开发与运行基础部分

(1) 需求分析和设计，包括需求分析和管理、结构化分析与设计、面向对象分析与设计、模块设计、I/O 设计、人机界面设计。

(2) 测试评审方法，包括测试方法、评审方法、测试设计和管理方法(注入故障、系统测试)。

(3) 项目管理基础知识，包括制订项目计划、质量控制计划、管理和评估、过程管理(PERT 图、甘特图、工作分解结构、进度控制、关键路径)、配置管理、人员计划和管理、文档管理、成本管理和风险管理。

(4) 系统维护，包括维护的类型、维护过程管理、硬件维护、软件维护。

4. 标准化和信息化部分

(1) 标准，包括国际标准(ISO、IEC)与美国标准(ANSI)、国家标准(GB)、行业标准与企业标准。

(2) 安全性标准，包括信息系统安全措施、CC 标准、BS 7799 标准等。

(3) 标准化组织，包括国际标准化组织、美国标准化组织、欧洲标准化组织、中国国家标准化委员会。

(4) 全球信息化趋势、国家信息化战略、企业信息化战略和策略、互联网相关的法律法规知识。

(5) 个人信息保护规则。

(6) 远程教育、电子商务、电子政务等基础知识。

(7) 企业信息化资源管理基础知识。

12.1.2　考点统计

“计算机基础知识”知识模块在历次网络工程师考试试卷中出现的考核知识点及分值分布情况如表 12.1 所示。

表 12.1　历年考点统计表

年　份	题　号	知 识 点	分　值
2017 年下半年	上午：1～10	Cache 与主存的地址映像、流水线技术、主存储器、输入输出系统、知识产权、PERT 图、软件开发方法论	10 分
	下午：无	无	0 分
2017 年上半年	上午：1、2、4、5、7～10	CPU、系统可靠性基础、PERT 图、知识产权	8 分
	下午：无	无	0 分
2016 年下半年	上午：1～10	CPU、指令系统、浮点数、海明码、流水线技术、PERT 图、PV 操作、知识产权	10 分
	下午：无	无	0 分
2016 年上半年	上午：1～10	内存、总线系统、知识产权、文件系统、输入输出系统	10 分
	下午：无	无	0 分
2015 年下半年	上午：1～10	直接存储器存取方式、虚拟存储器、寻址方式、内存编址、软件项目人员管理、PERT 图、文件系统、知识产权	10 分
	下午：无	无	0 分
2015 年上半年	上午：1～9	定点小数、CPU、中断、流水线技术、页面置换算法、著作权的归属	9 分
	下午：无	无	0 分

续表

年　份	题　号	知 识 点	分　值
2014 年下半年	上午：1～10	运算器与控制器、主存储器、Flynn 分类、软件开发方法论、PERT 图、产权人的确定	10 分
	下午：无	无	0 分
2014 年上半年	上午：1～10	CPU、定点表示法、流水线技术、主存储器、项目开发、相对路径和绝对路径、软件开发理论、产权人的确定	10 分
	下午：无	无	0 分
2013 年下半年	上午：1～10	Cache 与主存的地址映像、指令寄存器、逻辑运算、PERT 图、引用调用、学术论文中的引用、按字节编址、视频信息的基本概念	20 分
	下午：无	无	0 分
2013 年上半年	上午：1～6	存储器、中断向量、堆栈、内存访问模式、按字节编址	12 分
	下午：无	无	0 分
2012 年下半年	上午：1～4	控制器、主存储器、数的表示方法、 逻辑运算	8 分
	下午：无	无	0 分
2012 年上半年	上午：2～4	按字节编址、相联存储器、寻址方式	6 分
	下午：无	无	0 分

12.1.3　命题特点

纵观历年试卷，本章知识点是以选择题的形式出现在试卷中的。本章知识点在历次考试上午试卷中，所考查的题量大约为 10 道选择题，所占分值为 10 分(约占试卷总分值 75 分中的 17%)。本章考题主要检验考生是否理解相关的理论知识点，考试难度较低。

12.2　考点串讲

12.2.1　计算机硬件基础

计算机硬件通常由运算器、控制器、主存储器、输入设备和输出设备五大部件组成。其中把运算器和控制器合称为中央处理器，简称 CPU；把中央处理器和主存储器合称为主机。运算器是对数据加工处理的部件，它主要完成算术和逻辑运算。控制器的主要功能是从主存中取出指令，并指出下一条指令在主存中的位置。取出的指令经指令寄存器送往指令译码器，经过对指令的分析发出相应的控制和定时信息，控制计算机的各个部件有条不紊地工作，以完成指令所规定的操作。存储器是计算机系统中的记忆设备，用来存放程序、原始数据、中间结果及最终结果。输入设备的作用是把程序和原始数据转换成计算机中表示的二进制数，输入到计算机的主存中。输出设备的作用是把运算处理结果按照人们所要求的形式输出到外部存储介质上。

12.2.1.1　计算机中数据的表示

1. 机器数和码制

各种数据在计算机中的表示形式称为机器数，其特点是采用二进制计数制，数的符号用 0、1 表示，小数点则隐含表示而不占位置。真值是机器数所代表的实际数值。

机器数有无符号数和带符号数两种。无符号数表示正数，没有符号位。对无符号数，若约定小数点的位置在机器数的最低位之后，则是纯整数；若约定小数点的位置在最高位之前，则是纯小数。带符号数的最高位是符号位，其余位表示数值，同样，若约定小数点的位置在机器数的最低位之后，则是纯整数；若约定小数点的位置在最高数值位之前(符号位之后)，则是纯小数。

为方便运算，带符号的机器数可采用原码、反码和补码等不同的编码方法，这些编码方法称为码制。

1) 原码表示法

数值 X 的原码记为 $[X]_{原}$，最高位为符号位，表示该数的符号，“0”表示正数，“1”表示负数，而数值部分仍保留着其真值的特征。

2) 反码表示方法

反码的符号表示法与原码相同。正数的反码与正数的原码形式相同；负数的反码符号位仍为 1，数值部分通过将负数原码的数值部分各位取反(0 变 1，1 变 0)得到。

3) 补码表示法

正数的补码与原码相同，负数的补码是反码末位+1(丢弃最高位向上的进位)，它是最适合进行数字加减运算的数字编码。

2. 定点数和浮点数

实际处理的数既有整数部分又有小数部分，根据小数点位置是否固定，有两种表示格式：定点格式和浮点格式。

1) 定点表示法

定点表示法就是约定小数点的位置固定不变。小数点可以约定在数中的任何位置上，通常将小数点固定在符号位之后或整个数据的末位之后，也即将数据表示成纯小数或纯整数。定点数的运算规则比较简单，但不适宜对数值范围变化比较大的数据进行运算。

2) 浮点表示法

浮点表示法就是小数点的位置不固定，可根据需要左右浮动。在计算机中，一个任意进制数 N，其浮点数的真值为

$$N = \pm R^{E} M$$

其中：M 表示尾数；E 表示指数；R 表示基数。基数一般取 2、8、16。一旦机器定义好基数值，就不能再改变。因此，在浮点数表示中基数不出现，是隐含的。

3. 校验码

通常使用校验码的方法来检测传送的数据是否出错。其基本思想是把数据可能出现的编码分为两类：合法编码和错误编码。合法编码用于传送数据，错误编码是不允许在数据中出现的编码。

校验码中有一个重要概念——码距。所谓码距，是指一个编码系统中任意两个合法编码之间至少有多少个二进制位不同。

1) 奇偶校验码

奇偶校验通过在编码中增加一位来使编码中 1 的个数为奇数(奇校验)或者偶数(偶校验)，从而使码距变为 2。

2) 海明码

海明码是利用奇偶性来检错和校验的方法。其构成方法是：在数据位之间插入 *k* 个校验位，通过扩大码距来实现检错和纠错。

3) 循环冗余校验码

循环冗余校验码(CRC)由两部分组成，左边为信息码(数据)，右边为校验码。若 CRC 码的字长为 *n*，信息码占 *k* 位，则校验码就占 *n*−*k* 位。校验码是由信息码产生的，校验位越长，校验能力就越强。在求 CRC 编码时，采用的是模 2 运算。

12.2.1.2 中央处理器(CPU)

中央处理器，即 CPU，是运算器和控制器的合称。

1. CPU 的功能

(1) 程序控制：CPU 通过执行指令来控制程序的执行顺序。

(2) 操作控制：一条指令功能的实现需要若干操作信号来完成，CPU 产生每条指令的操作信号并将其送往不同的部件，控制相应部件的操作。

(3) 时序控制：CPU 通过时序电路产生的时钟信号进行定时，以控制各种操作按指定时序进行。

(4) 数据处理：完成对数据的加工处理。

2. CPU 的组成

1) 运算器

运算器主要完成算术运算、逻辑运算和移位操作，其主要部件有算术逻辑单元 ALU、累加器 ACC、标志寄存器、寄存器组、多路转换器和数据总线等。

2) 控制器

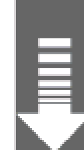
控制器实现指令的读入、寄存、译码和在执行过程有序地发出控制信号。控制器主要由指令寄存器 IR、程序计数器 PC、指令译码器、状态/条件寄存器、时序产生器、微操作信号发生器组成。

3) 寄存器

寄存器用于暂存寻址和计算过程的信息。CPU 中的寄存器通常分为存放数据的寄存器、存放地址的寄存器、存放控制信息的寄存器、存放状态信息的寄存器和其他寄存器等类型。

3. 流水线技术

流水线技术把 CPU 的一个操作进一步分解成多个可以单独处理的子操作(如取指令、指令译码、取操作数、执行)，使每个子操作在一个专门的硬件站上执行，这样一个操作需要顺序地经过流水线中多个站的处理才能完成。在执行的过程中，前后连续的几个操作可以依次流入流水线中，在各个站间重叠执行。其工作原理如图 12.1 所示。



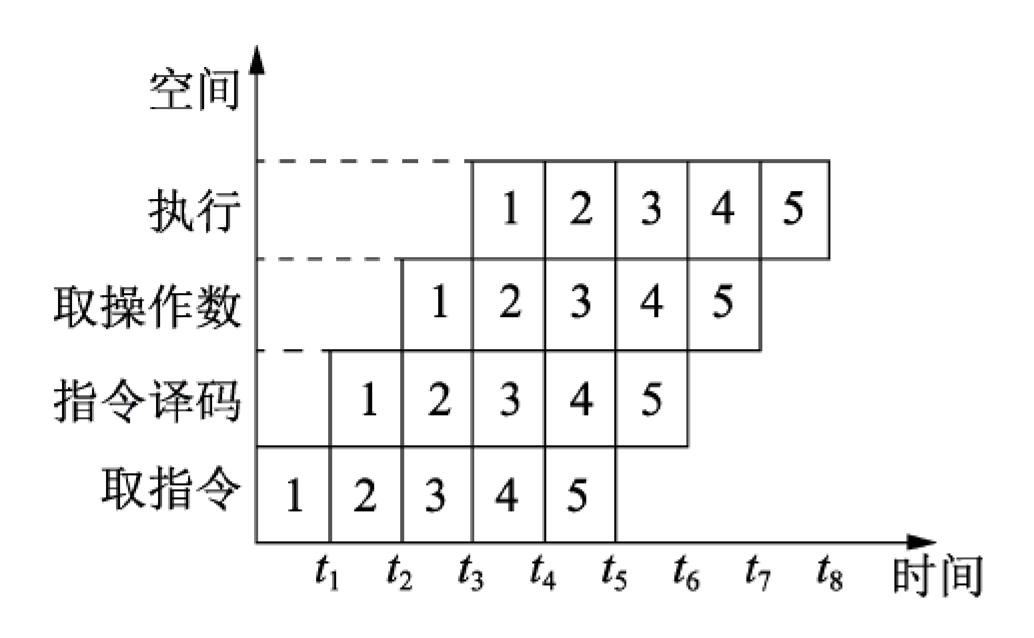


图 12.1　流水线技术

设某流水线技术分为 n 个基本操作，操作时间分别是 $\Delta t_i (i=1,2,\cdots,n)$。

(1) 操作周期：取决于基本操作时间最长的一个，即操作周期为

$$\Delta t = \max\{\Delta t_1, \Delta t_2, \cdots, \Delta t_i\}$$

(2) 吞吐率：流水线的吞吐率为

$$p = 1/\Delta t = 1/\max\{\Delta t_1, \Delta t_2, \cdots, \Delta t_i\}$$

(3) 流水线的建立时间：即第一条指令完成的时间。

$$T_1 = n \times \Delta t = n \times \max\{\Delta t_1, \Delta t_2, \cdots, \Delta t_i\}$$

(4) 执行 m 条指令的时间：

$$T = n \times \Delta t + (m-1) \times \Delta t = (n+m-1) \times \max\{\Delta t_1, \Delta t_2, \cdots, \Delta t_i\}$$

或

$$T = \sum_{i=1}^{n} \Delta t_i + (m-1) \times \Delta t = \sum_{i=1}^{n} \Delta t_i + (m-1) \times \max\{\Delta t_1, \Delta t_2, \cdots, \Delta t_i\}$$

12.2.1.3　存储系统

1. 主存储器

主存储器简称内存或主存，用来存放当前正在使用或随时要使用的数据和程序，CPU 可直接访问。主存一般由 RAM 和 ROM 这两种工作方式的存储器组成，其绝大部分存储空间由 RAM 构成。

主存储器的性能指标包括以下几个方面。

(1) 存储容量：每个内存储单元都有一个地址，对内存的读、写操作都要给出地址来选择具体单元。在微机系统中内存是以字节作为一个单元的，在不同字长的系统中，一次可以对 2 个、4 个或 8 个单元访问。存储容量用字数或字节数(B)来表示，如 64KB、512KB、10MB。

(2) 存取时间：从启动一次存储器操作到完成该操作所经历的时间。

(3) 存储周期：连续启动两次独立的存储器操作(如连续两次读操作)所需间隔的最小时间。通常，存储周期略大于存储时间，其时间单位为 ns。

(4) 存储器带宽：每秒钟能访问的 bit 数，记作 B_m。设每个存取周期存取数据位为 W_b，则 $B_m=W_b/T_m$。

2. 存储器的构成

存储器芯片的容量是有限的，其字数或字长与实际存储器的要求都有很大差距，我们可以从字向和位向两个方面对存储器的容量进行扩充。假设一个存储器的容量为 $M\times N$ 位，若使用 $m\times n$ 位的芯片($m\leqslant M$，$n\leqslant N$)，共需要$(M/m)\times(N/n)$个存储器芯片。

3. 相关联存储器

相关联存储器(CAM)是一种按内容寻址的存储器。其工作原理就是把数据或数据的某一部分作为关键字，将该关键字与存储器中的每一单元进行比较，找出存储器中所有与关键字相同的数据。

4. Cache

Cache 即高速缓冲存储器，为了解决 CPU 和主存之间速度匹配问题而设置。它是介于 CPU 和主存之间的小容量存储器，存取速度比主存快。其改善系统性能的依据是程序的局部性原理。

- Cache 主要由两部分组成：控制部分和存储器部分。
- Cache 存储器部分用来存放主存的部分复制。
- 控制部分的功能是判断 CPU 要访问的信息是否在 Cache 存储器中，若在即为命中，若不在则没有命中。

5. 性能分析

(1) 命中率：在 Cache 中访问到信息的概率，一般用模拟实验的方法得到。选择一组有代表性的程序，在程序执行过程中分别统计对 Cache 的访问次数 N_1 和对主存的访问次数 N_2，则 Cache 的命中率为 $H = N_1/(N_1 + N_2)$。

(2) 平均实际存取时间：可以用 Cache 和主存的访问周期 T_1、T_2 以及命中率 H 来表示，即 $T = H \cdot T_1 + (1-H) \cdot T_2$。当命中率 $H \to 1$ 时，$T \to T_1$，即平均实际存取时间 T 接近于速度比较快的 Cache 的访问周期 T_1。

(3) 访问效率：访问效率为 $e = T_1/T$。

6. 地址映像

当 CPU 访问内存时，用的是访问主存的地址，由该地址变为访问 Cache 的地址称为“地址变换”。变换过程采用硬件来实现，以达到快速访问的目的。地址映像方式有：全相联方式、直接方式和组相联方式。

7. 磁盘存储器

磁盘存储器是外存中最常用的存储介质，存取速度较快且具有较大的存储容量，分为软盘和硬盘存储器。

12.2.1.4 输入输出系统

1. I/O 接口

接口又称为界面，是指两个相对独立的子系统之间的相连部分。用于连接主机和 I/O 设备的这个转换机构就是 I/O 接口电路。

接口有多种分类方法，具体如下。

(1) 按数据的传送格式，接口可分为并行接口和串行接口。

(2) 按主机访问 I/O 设备的控制方式，接口可分为程序查询接口、中断接口、DMA 接口以及通道控制器、I/O 处理机等。

(3) 按时序控制方式，接口可分为同步接口和异步接口。



2. 接口的控制方式

1) 直接程序控制

(1) 程序查询方式。

在这种方式下，CPU 通过执行程序查询外设的状态，判断外设是否准备好进行数据传送。

(2) 立即程序传送方式。

在这种方式下，I/O 接口总是准备好接收来自主机的数据，或随时准备向主机输入数据，CPU 无须查看接口的状态，而直接执行输入/输出指令进行数据传送。这种方式又称为无条件传送或同步传送。

2) 中断方式

当出现来自系统外部、机器内部，甚至处理机本身的任何例外时，CPU 暂停执行现行程序，转去处理这些事件，等处理完成后再返回来继续执行原先的程序。

3) DMA 方式

DMA(直接存储器存取)方式不是用软件而是采用一个专门的控制器来控制内存与外设之间的数据交流，无须 CPU 介入，可大大提高 CPU 的工作效率。

4) I/O 通道

通道又称输入/输出处理器(IOP)，目的是使 CPU 摆脱繁重的输入输出负担和共享输入输出接口，多用于大型计算机系统中。根据多台外围设备共享通道的不同情况，可将通道分为 3 种类型：字节多路通道、选择通道和数组多路通道。

12.2.1.5　总线系统

1. 总线的定义与分类

总线是连接多个设备的信息传送通道，是一组信号线，一般可分为芯片内总线、元件级总线、内总线、外总线。

1) 内总线

内总线又称系统总线，是计算机各组成部分(CPU、内存和外设接口)间的连接。系统总线按功能可分为 3 类：地址总线、数据总线、控制总线。

常见的内总线标准有以下几种。

- ISA(Industry Standard Architecture)总线：数据线有 16 位，地址线有 24 位。
- EISA(Enhanced Industry Standard Architecture)总线：EISA 总线是 ISA 总线的扩展，现用在服务器上。数据线有 32 位，与 ISA 总线兼容。
- PCI(Peripheral Computer Interconnect)总线：目前微型机上广泛采用的内总线。PCI 总线的工作与处理机的工作是并行的。PCI 总线上的设备是可即插即用的。

2) 外总线

外总线又称通信总线，是计算机对外的接口，可直接与相应的外设连接或与其他计算机相连接。常见的外总线标准有以下几种。

- 串行总线接口(RS-232)：国际通用的一种串行通信接口标准。
- SCSI(Small Computer System Interface)总线：一条并行外部总线，广泛用于连接软硬磁盘、光盘、扫描仪等。
- 通用串行总线(Universal Serial Bus，USB)：USB 接口提供电源，最大数据传输率

为 12 Mb/s，支持即插即用功能。

- IEEE 1394(Firewire)：由 6 条信号线组成，可连接设备数多，传输速度快，支持即插即用功能。

2. 总线的指标

(1) 总线宽度：一次可以传输数据的位数，S100 为 8 位，ISA 为 16 位，EISA 为 32 位，PCI-2 可达 64 位。总线宽度不会超过微处理器外部数据总线的宽度。

(2) 总数工作频率：总线信号中有一个 CLK 时钟信号，CLK 越高，每秒钟传输的数据量越大。ISA、EISA 为 8 MHz，PCI 为 33.3 MHz，PCI-2 为 66.6 MHz。

(3) 单个数据传输周期：不同的传输方式，每个数据传输所用 CLK 周期数不同。ISA 用 2 个周期，PCI 用 1 个周期。这决定总线最高数据传输率。

12.2.1.6 指令系统

1. 指令

指令是指挥计算机完成各种操作的基本命令。

(1) 指令格式：计算机的指令由操作码字段和操作数字段两部分组成。

(2) 指令长度：指令长度有固定长度和可变长度两种。有些 RISC 的指令是固定长度的，但目前多数计算机系统的指令是可变长度的。指令长度通常取 8 的倍数。

(3) 指令种类：数据传送指令、算术运算指令、位运算指令、程序流程控制指令、串操作指令、处理器控制指令。

2. 寻址方式

寻址方式可分为以下几种。

(1) 立即寻址：操作数作为指令的一部分而直接写在指令中，这种操作数称为立即数。

(2) 寄存器寻址：指令所要的操作数已存储在某寄存器中，或把目标操作数存入寄存器。

(3) 直接寻址：指令所要的操作数存放在内存中，在指令中直接给出该操作数的有效地址。

(4) 寄存器间接寻址：操作数在存储器中，操作数的有效地址用 SI、DI、BX 和 BP 等 4 个寄存器之一来指定。

(5) 寄存器相对寻址：操作数在存储器中，其有效地址是一个基址寄存器(BX、BP)或变址寄存器(SI、DI)的内容和指令中的 8 位/16 位偏移量之和。

(6) 基址加变址寻址方式：操作数在存储器中，其有效地址是一个基址寄存器(BX、BP)和一个变址寄存器(SI、DI)的内容之和。

(7) 相对基址加变址寻址：操作数在存储器中，其有效地址是一个基址寄存器(BX、BP)的值、一个变址寄存器(SI、DI)的值和指令中的 8 位/16 位偏移量之和。

3. 复杂指令集计算机

在计算机发展的早期，计算机技术水平较低，硬件较为简单，由硬件实现的指令系统的功能也就简单，一般只有定点的加减及逻辑运算、数据传送和程序转移等数十条最基本的指令。随着计算机逻辑元件的迅猛发展，特别是超大规模集成电路的发展，机器的造价、体积、功耗及可靠性等方面都有了长足的发展。同时，随着计算机应用领域的日益扩大，

对指令系统功能的要求越来越高，使指令系统逐渐发展到几百种，寻址方式也更加灵活多样，具备这种指令系统的计算机称为复杂指令集计算机(Complex Instruction Set Computer，CISC)。

4. 精简指令集计算机

在指令系统中只有大约 20%的最简单的指令被经常使用，其使用频度达 80%。若只保留 20%的最简单的指令，使指令尽可能简单，从而设计一种硬件结构十分简单、执行速度很高的 CPU，这就是精简指令集计算机(RISC)。

12.2.1.7　系统可靠性基础

1. 基本概念

(1) 系统的可靠性：从它开始运行(t=0)到某时刻 t 这段时间内能正常运行的概率，用 $R(t)$ 表示。

(2) 失效率：单位时间内失效的元件数与元件总数的比例，通常用λ表示。当λ为常数时，可靠性与失效率的关系为 $R(t)=e^{-\lambda t}$ 。

(3) 平均无故障时间(MTBF)：两次故障之间系统能正常工作的时间的平均值。它与失效率的关系为 $\text{MTBF}=1/\lambda$ 。

(4) 平均失效前时间(MTTF)：从故障发生到机器修复平均所需要的时间。通常用平均修复时间(MTTR)来表示计算机的可维修性，即计算机的维修效率。

(5) 可用性：计算机的使用效率。它以系统在执行任务的任意时刻能正常工作的概率 A 来表示，即 $A=\text{MTBF}/(\text{MTBF}+\text{MTTR})$ 。

2. 系统可靠性模型

(1) 串联系统：假设一个系统由 N 个子系统组成，当且仅当所有的子系统都能正常工作时，系统才能正常工作。

(2) 并联系统：假如一个系统由 N 个子系统组成，只要有一个子系统正常工作，系统就能正常工作。

(3) N 模冗余系统：由 N 个(N=2n+1)相同的逻辑线路和一个表决器组成，只要有 n+1 个或 n+1 个以上能正常工作，系统就能正常工作，输出正确的结果。

12.2.2　操作系统

12.2.2.1　操作系统的基本概念

操作系统(Operating System，OS)是计算机系统中的一个系统软件，它能有效地组织和管理系统中的各种硬件和软件资源，合理地组织计算机系统的工作流程，控制程序的执行，并向用户提供一个良好的工作环境和友好的接口。

操作系统主要有并发性(Concurrency)、共享性(Sharing)、虚拟性(Virtual)和不确定性(Non-Determinacy)4 个基本特征。

1. 操作系统的功能

操作系统的功能如下。

(1) 进程管理：包括进程控制、进程通信和进程调度。

(2) 存储管理：包括存储分配和回收、存储保护、地址映射和主存扩充。

(3) 设备管理：包括对输入输出设备的分配、启动、完成和回收。

(4) 文件管理：包括文件存储空间管理、目录管理、文件的读写管理和存取控制。

(5) 作业管理：包括任务、界面管理、人机交互、图形界面、语音控制和虚拟现实等。

2. 操作系统的分类

根据操作系统的使用环境和对作业的处理方式来划分，操作系统的基本类型有：批处理操作系统、分时系统、实时系统、网络操作系统、分布式操作系统、微机操作系统、嵌入式操作系统。

12.2.2.2　处理机管理

1. 进程的基本概念

进程是一个程序在一个数据集合上的一次执行，是操作系统中可以并行工作的基本单位，也是核心调度及资源分配的最小单位，它由程序、数据、进程控制块(PCB)组成。进程与程序的重要区别之一是：进程是有状态的，而程序没有，程序是静态的。

进程的基本特征有：动态性、并发性、独立性、异步性、结构特征。

传统上，每个进程在任何时刻总是处于 3 种基本状态(即运行、就绪、阻塞)的某一种基本状态。在不少系统中，还增加了两种基本状态：新建态、终止态。状态之间的转换如图 12.2 所示。

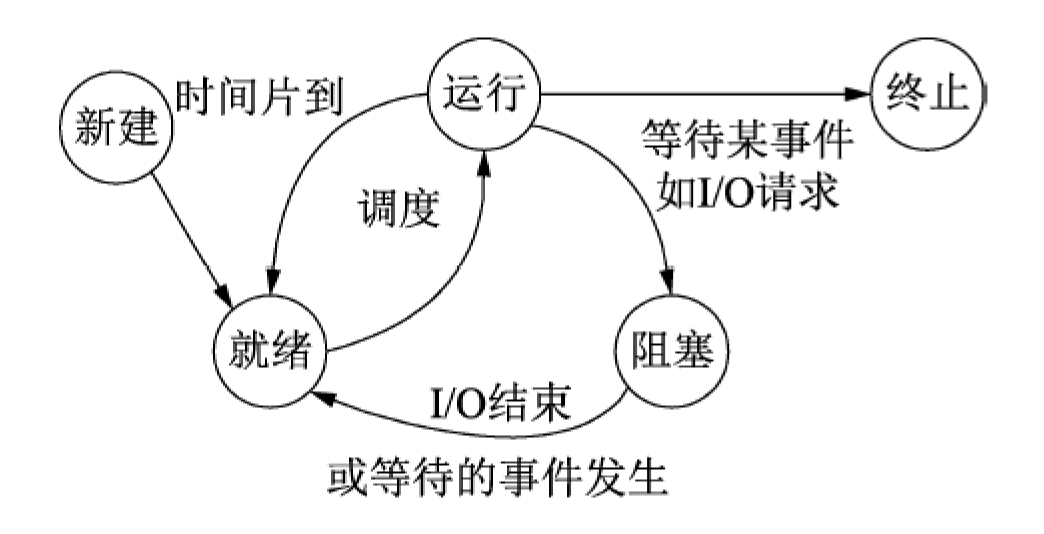


图 12.2　进程状态转换图

2. 线程

在 SMP(对称多处理)系统中，操作系统还提供了线程机制。线程是比进程更小的能独立运行的基本单位，它是处理器分配的最小单位。

进程是资源分配的基本单位，而线程与资源分配无关，它属于某一个进程，并与进程内的其他线程一起共享进程的资源。线程也有就绪、阻塞和执行 3 种基本状态。

3. 进程间通信

1) 同步与互斥

(1) 进程间的同步。

一个进程相对于另一个进程的运行速度是不确定的，也就是说进程是在异步环境下运

行的。每个进程都以各自独立的、不可预知的速度向前推进。但相互合作的进程需要在某些确定点上协调它们的工作，当一个进程到达了这些点后，除非另一进程已经完成了某些操作，否则就不得不停下来等待这些操作结束。

(2) 进程间的互斥。

在多道程序系统中，各进程可以共享各类资源，但有些资源一次只能供一个进程使用，称为临界资源(Critical Resource，CR)，例如打印机、公共变量和表格等。同步是进程间的直接制约问题，互斥是进程间的间接制约问题。

2) 信号量机制

信号量是一种解决进程同步与互斥的工具，主要有整型信号量、记录型信号量、信号量集机制。最常用的信号量是整型变量。

信号量可分为两类：一类是公用信号量，用于实现进程间的互斥，初值等于 1 或资源的数目；另一类是私用信号量，用于实现进程间的同步，初值等于 0 或某个正整数。信号量 S 的物理意义是：当 $S \geqslant 0$ 时，表示某资源的可用数；当 $S<0$ 时，其绝对值表示阻塞队列中等待该资源的进程数。

3) P、V 操作

PV 操作是实现进程同步与互斥的常用方法，PV 操作是低级通信原语，在执行期间不可分割。其中，P 操作表示申请一个资源，V 操作表示释放一个资源。

P 操作定义：$S=S-1$，若 $S \geqslant 0$，则执行 P 操作的进程继续执行；否则，若 $S<0$，则置该进程为阻塞状态(因为无可用资源)，并将其插入阻塞队列。

V 操作定义：$S=S+1$，若 $S>0$，则执行 V 操作的进程继续执行；否则，若 $S \leqslant 0$，则从阻塞状态唤醒一个进程，并将其插入就绪队列，执行 V 操作的进程继续执行。

利用 PV 操作实现进程互斥的方法为：令信号量 mutex 的初值为 1，当进程进入临界区时执行 P 操作，退出临界区时执行 V 操作。

利用 PV 操作实现进程同步的方法为：用一个信号量与消息联系起来，当信号量的值为“0”时表示希望的消息未产生，当信号量的值为非“0”时表示希望的消息已经存在。假定用信号量 S 表示某条消息，进程可以通过调用 P 操作测试消息是否到达，调用 V 操作通知消息已准备好。最典型的就是单缓冲区的生产者和消费者的同步问题。

4. 进程调度算法

(1) 先来先服务调度算法：按进程进入就绪队列的先后次序选择可以占用处理器的进程。

(2) 优先数调度算法：对每个进程确定一个优先数，进程调度总是让具有最高优先数的进程先使用处理器。如果进程具有相同的优先数，则对这些有相同优先数的进程再按先来先服务的次序分配处理器。

(3) 时间片轮转调度算法：把规定进程一次使用处理器的最长时间称为时间片。让就绪进程按就绪的先后次序排成队列，每次总是选择就绪队列中的第一个进程占用处理器，但规定只能使用一个时间片。如果一个时间片用完，进程工作尚未结束，则它也必须让出处理器给其他进程使用，自己被重新排到就绪队列的末尾，等待再次运行。时间片轮转调度算法经常用在分时操作系统中。

(4) 分级调度算法：由系统设置多个就绪队列，每个就绪队列中的进程按时间片轮转法

占用处理器。

5. 死锁

1) 产生死锁的原因

若系统中存在一组进程，它们中的每个进程都占用了某种资源，而又都在等待其中另一个进程所占用的资源，这种等待永远不能结束，则说明系统出现了死锁。只要下面 4 个条件中有一个不具备，系统就不会出现死锁。

(1) 互斥条件。某个资源在一段时间内只能由一个进程占有，不能同时被两个或两个以上的进程占有。

(2) 不可抢占条件。进程所获得的资源在未使用完毕之前，资源申请者不能强行地从资源占有者手中夺取资源，而只能由该资源的占有者进程自行释放。

(3) 占有且申请条件。进程至少已经占有一个资源，但又申请新的资源，由于该资源已被另外进程占有，此时该进程阻塞，但是，它在等待新资源之时，仍继续占用已占有的资源。(注：也称为保持与等待条件)

(4) 循环等待条件。存在一组进程等待序列$\{P_1,P_2,\cdots,P_n\}$，其中 P_1 等待 P_2 所占有的某一资源，P_2 等待 P_3 所占有的某一资源，……，而 P_n 等待 P_1 所占有的某一资源，形成一个进程循环等待环。

2) 死锁的预防方法

死锁的预防方法如下。

(1) 打破互斥条件。

(2) 打破不可抢占条件。

(3) 打破占有且申请条件。

12.2.2.3 存储管理

1. 分页存储管理

1) 分页原理

将一个进程的地址空间划分成若干大小相等的区域，称为页。相应地，将主存空间划分成与页相同大小的若干物理块，称为块或页框架。在为进程分配主存时，将进程中若干页分别装入多个不邻接的块中。

2) 地址结构

地址结构由两部分组成：前一部分为页号 P；后一部分为偏移量 W，即页内地址。图 12.3 中的地址长度为 32 位，其中 0～11 位为页内地址(每页的大小为 4 KB)，12～31 位为页号，所以允许地址空间的大小最多为 1 MB 个页。

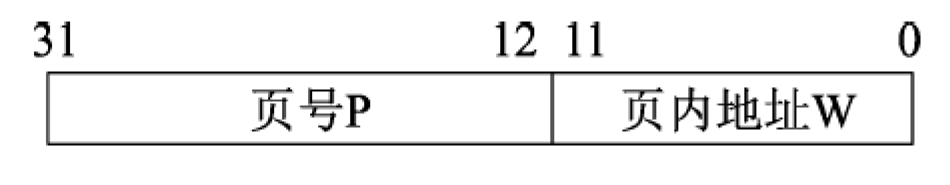


图 12.3　分页地址结构

3) 地址变换

系统为每个进程建立了一张页面映射表，简称页表。每个页在页表中占一个表项，记录该页在内存中对应的物理块号。进程在执行时，通过查找页表，就可以找到每页所对应的物理块号。可见，页表的作用是实现从页号到物理块号的地址映射。

2. 分段存储管理

1) 分段基本原理

作业的地址空间被划分为若干段，每个段定义了一组逻辑信息。每个段都有自己的名字，都是从零开始编址的一段连续的地址空间，段的长度由相应逻辑信息组的长度决定，因而各段长度不等，整个作业的地址空间是二维的。分段系统中地址结构如图 12.4 所示，其逻辑地址由段号(名)和段内地址两部分组成，在该地址结构中，允许一个作业最多能有 256 个段，每个段的最大长度为 64KB。

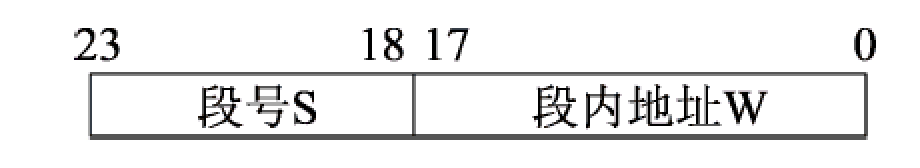


图 12.4　分段地址结构

2) 地址变换机构

在分段式存储管理系统中，为每个段分配一个连续的分区，而进程中的各个段可以离散地分配到内存中不同的分区中。在系统中为每个进程建立一张段映射表，简称为“段表”。进程在执行中，通过查段表来找到每个段所对应的内存区。所以说，段表实现了从逻辑段到物理内存区的映射。

3. 虚拟存储管理

1) 局部性原理

局部性原理是虚拟存储技术的理论基础，是指程序的执行往往呈现出高度的局限性，即程序执行时往往会不均匀地访问内存储器。程序的局限性表现在以下两个方面。

- 时间局部性：若一条指令被执行，则在不久的将来，它可能再被执行。
- 空间局部性：一旦一个存储单元被访问，那么它附近的单元也将很快被访问。

2) 虚拟存储器的定义

利用大容量的外存(通常是高速硬盘)来扩充内存，产生一个比有限的实际内存空间大得多的、逻辑的虚拟内存空间，以便能够有效地支持多道程序系统的实现和大型作业运行的需要，从而增强系统的处理能力。当进程要求运行时，不是将它的全部信息装入内存，而是将其一部分先装入内存，另一部分暂时留在外存。进程在运行过程中，要使用的信息不在内存时发生中断，由操作系统将它们调入内存，以保证进程的正常运行。从用户角度看，该系统所具有的主存容量，将比实际主存容量大得多，人们把这样的存储器称为虚拟存储器。

3) 虚拟存储器的实现

- 请求分页系统：在分页系统的基础上，增加了请求调页功能和页面置换功能所形成的页式虚拟存储系统。请求分页机制是在纯分页的页表机制上形成的，由于只将应用程序的一部分调入主存，还有一部分仍在磁盘上，故需在页表中再增加若干项，如状态位、访问字段、辅存地址等供程序(数据)在换进、换出时引用。在请求分页系统中，每当所要访问的页面不在主存时，便要产生一个缺页中断，请求操作系统将所缺页调入主存。它与一般中断的主要区别在于缺页中断在指令执行期间产生和处理中断信号，而一般中断在一条指令执行完后检查和处理中断信号；缺页中断返回到该指令的开始重新执行该指令，而一般中断返回到该指令的下一条指令执行。
- 请求分段系统：在分段系统的基础上，增加了请求调段功能和分段置换功能所形

成的段式虚拟存储系统。

4) 替换算法

- 最佳置换算法(OPT)：OPT 是一种理论化的算法。该算法淘汰在访问串中将来再也不出现的或是在最长时间内不再访问的页，这样，淘汰掉的页将不会造成因需要访问该页又需要把它调入的现象。这种最佳策略本身不是一种实际的方法，它的理论价值在于用 OPT 算法的缺页率去评价其他算法的优劣。
- 先进先出算法(FIFO)：FIFO 总是选择作业中在主存驻留时间最长(即最老)的一页淘汰，即先进入主存的页先退出主存。其理由是，最早调入主存的页，其不再被使用的可能性比最近调入主存的页要大。
- 最近最久未使用置换算法(LRU)：LRU 选择在最近一段时间内最久不用的页予以淘汰。这是最常用的页面置换算法。
- 最近未用置换算法(NUR)：NUR 是将最近一段时间未引用过的页面换出。它是一种 LRU 的近似算法。

12.2.2.4 设备管理

1. DMA 与缓冲技术

1) DMA 技术

DMA(Directed Memory Access)的基本思想是：在外围设备和主存之间开辟直接的数据交换通路，在内存与输入输出设备间传送一个数据块的过程中，不需要 CPU 的任何干涉，只需要 CPU 在过程开始启动与过程结束时的处理，实际操作由 DMA 硬件直接执行完成。

2) 缓冲技术

引入缓冲技术的目的是：缓和 CPU 和 I/O 设备间速度不匹配的矛盾；提高它们之间的并行性；减少对 CPU 的中断次数，放宽 CPU 对中断响应时间的要求。

缓冲技术可以采用硬件缓冲和软件缓冲两种。硬件缓冲是利用专门的硬件寄存器作为缓冲区；软件缓冲是利用操作系统的管理，用主存中的一个或多个区域作为缓冲区，进而可以形成缓冲池。

2. Spooling 系统

(1) Spooling 技术：用一类物理设备模拟另一类物理设备的技术，可以将低速的独占设备改造成一种可共享的设备，而且一台物理设备可以对应若干台虚拟的同类设备。Spooling 系统的引入缓和了 CPU 与设备速度的不均匀性，提高了 CPU 与设备的并行程度。

(2) Spooling 系统的组成：Spooling 系统由预输入程序、缓输出程序、井管理程序以及输入和输出井组成，如图 12.5 所示。

(3) Spooling 系统的工作过程：Spooling 系统将一个作业从进入系统到完成后撤离系统的全过程，划分成输入、处理和输出 3 个并发执行的过程。当用户作业要进入系统时，由 Spooling 系统的预输入程序将作业信息从物理输入设备送到磁盘上的指定区域(称为输入井)。输入井中的作业有以下 4 种状态。

- 输入状态：作业的信息正从输入设备上预输入。
- 收容状态：作业预输入结束但未被选中执行。
- 执行状态：作业已被选中运行过程中，它可从输入井中读取数据信息，也可向输



出井写信息。

- 完成状态：作业已经撤离，该作业的执行结果等待缓输出。

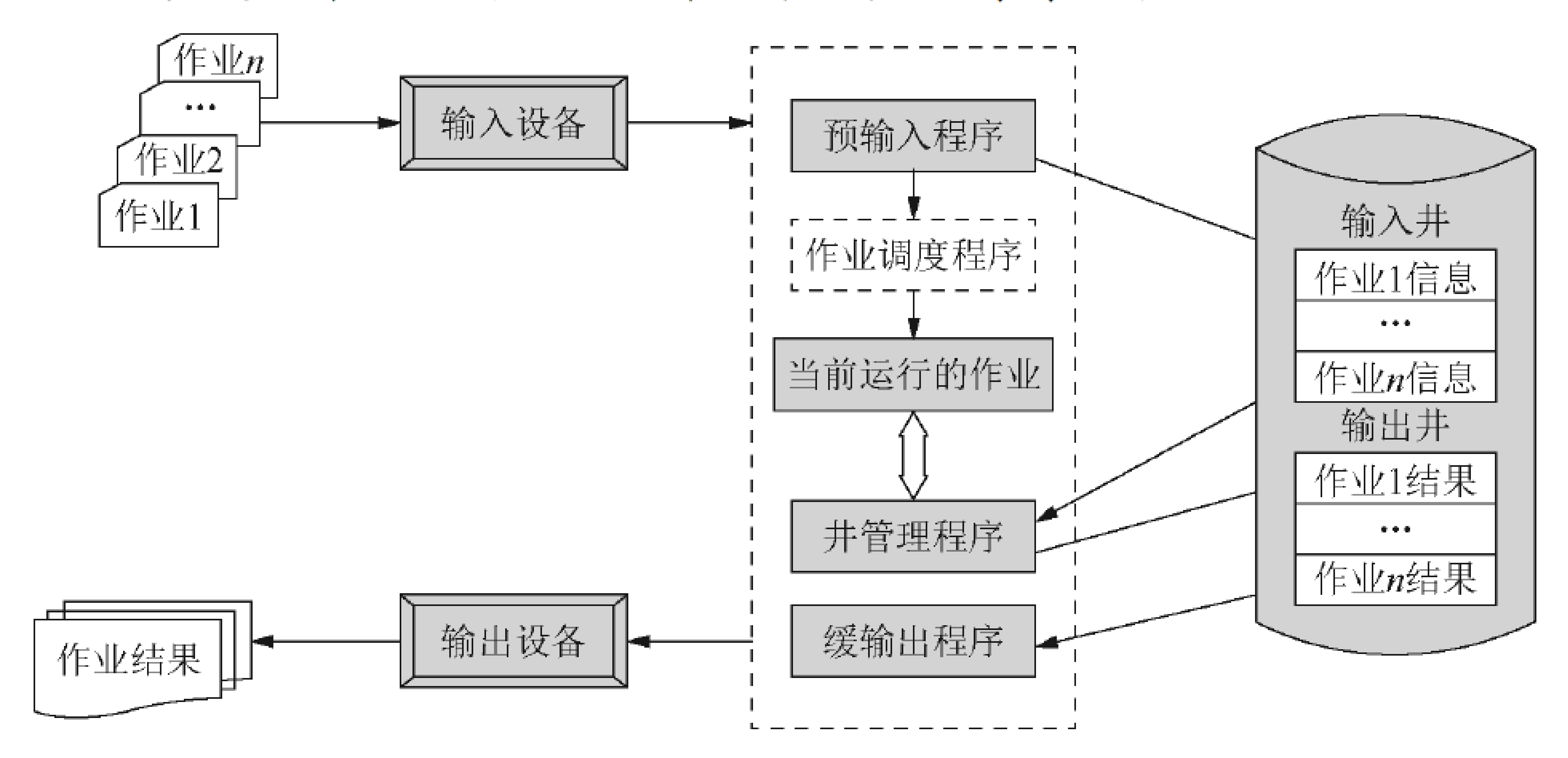


图 12.5　Spooling 系统的组成

12.2.2.5　文件管理

文件是信息的一种组织形式，是存储在辅助存储器上的具有标识名的一组集合。操作系统中由文件系统来管理文件的存储、检索、更新、共享和保护。文件系统包括两方面：一方面是负责管理文件的一组系统软件，另一方面是文件本身。

1. 文件类型

根据文件的性质和用途，文件有多种分类方法，具体如下。

- 按文件的用途，文件可以分为系统文件、库文件和用户文件等。
- 按信息保存期限，文件可分为临时文件、档案文件和永久文件。
- UNIX 系统将文件分为普通文件、目录文件和设备文件(特殊文件)等。
- 按文件的保护方式，文件可分为只读文件、读写文件、可执行文件和不保护文件等。

目前常用的文件系统类型有：FAT、VFAT、NTFS、Ext2、HPFS 等。

2. 文件的结构

文件的结构是指文件的组织形式，从用户观点所看到的文件组织形式，称为文件的逻辑结构；从实现观点考查文件在辅助存储器上的存放方式，常称为文件的物理结构。

(1) 逻辑结构分为两种：无结构的字符流文件和有结构的记录文件。记录文件由记录组成，即文件内的信息划分成多个记录，以记录为单位组织和使用信息。记录文件有顺序文件、索引顺序文件、索引文件和直接文件。

(2) 物理结构是文件在存储设备上的存放方法。常用的文件物理结构有：连续结构、链接结构、索引结构。

3. 文件目录

文件目录是文件控制块的集合，通常文件目录也被组织成文件，称为目录文件。文件系统一般采用一级目录结构、二级目录结构和多级目录结构。DOS、UNIX、Windows 系统

都是采用多级目录结构。

工作目录也称当前目录。在多级目录结构的文件系统中，文件的全路径名可能较长，也会涉及多次磁盘访问，为了提高效率，操作系统提供了设置工作目录的机制，每个用户都有自己的工作目录，任一目录节点都可以被设置为工作目录。一旦某个目录节点被设置成工作目录，相应的目录文件有关内容就会被调入主存，这样，对以工作目录为根的子树内任一文件的查找时间会缩短，从工作目录出发的文件路径名称为文件的相对路径名。文件系统允许用户随时改变自己的工作目录。

4. 存取方法和存取控制

1) 文件的存取方法

文件的存取方法是指读写文件存储器上的一个物理块的方法。通常有顺序存取、随机存取和按键存取等方式。

2) 文件存储空间的管理

文件存储空间的管理实质是对空闲块的组织和管理问题，它包括空闲块的组织、分配和回收等。常用的空间管理方法有位示图、空闲块表和空闲块链 3 种。

5. 文件的使用

一般文件系统提供一组专门用于文件、目录的管理，如目录管理、文件控制和文件存取等命令。

(1) 目录管理命令：如建立目录、显示工作目录、改变目录、删除目录(一般只可删除空目录)。

(2) 文件控制命令：如建立文件、删除文件、打开文件、关闭文件、修改文件名、改变文件属性。

(3) 文件存取命令：如读写文件、显示文件内容、复制文件等。

6. 文件的共享和保护

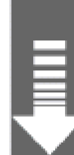
文件共享是指不同的用户使用同一文件。文件的共享可以采用文件的绝对路径名(或相对路径名)共享同一文件。保护是指避免文件拥有者或其他用户有意或无意地使文件受到破坏。这两个问题涉及用户对文件的访问权限，即文件的访问控制。常见的文件访问控制方式有访问控制矩阵、访问控制表、用户权限表、口令和密码。

文件的安全是指文件的保密和保护，即限制未授权用户使用或破坏文件，常常在系统级、用户级、目录级和文件级上实施。对目录和文件的访问权限可以由建立者设置。除了限定访问权限，建立者还可以通过加密等方式对文件进行保护。

12.2.2.6 作业管理

作业是用户在一次上机过程中，要求计算机所做的工作的集合。作业由程序、数据和作业说明书 3 部分组成。其中作业说明书包括作业基本情况、作业控制、作业资源要求的描述，它体现用户的控制意图。

作业控制块(JCB)是记录该作业的有关信息。JCB 是作业存在的唯一标志，主要包括：作业名、作业状态、资源要求、作业控制方式、作业类型以及作业优先级。



1. 作业的状态

作业的状态分为 4 种：提交、后备、执行和完成。它们之间的转换如图 12.6 所示。

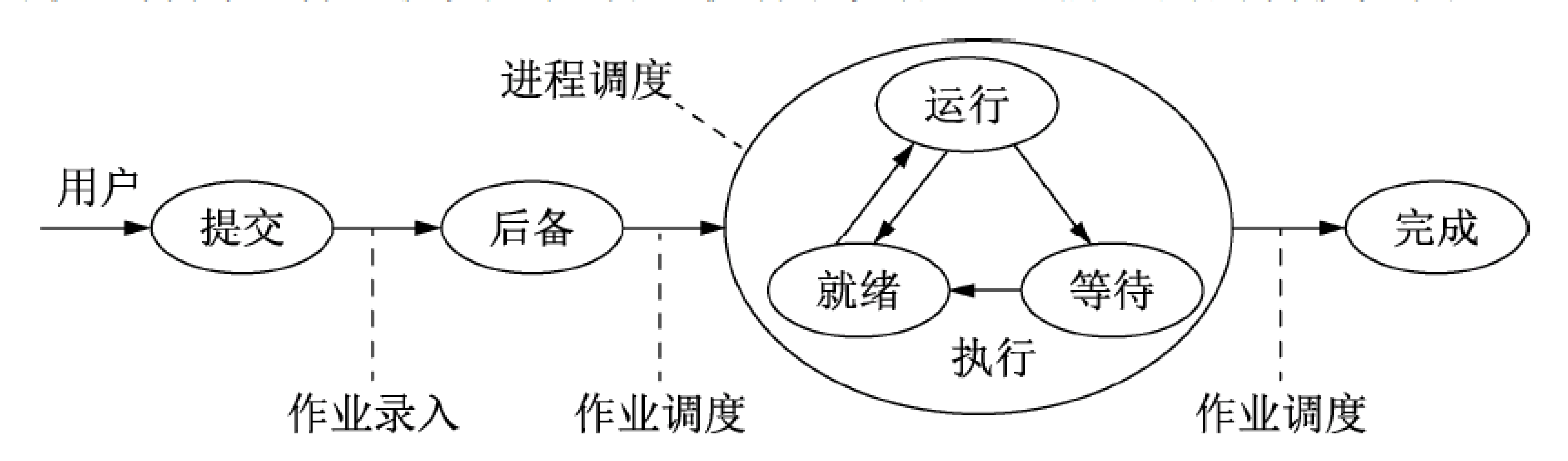


图 12.6　作业调度与进程调度

2. 作业调度算法

- 先来先服务(FCFS)：这是一种最简单的算法，它按照作业到达的先后次序来挑选作业，先进入的作业优先被挑选。
- 短作业优先(SJF)：作业的长短是以要求运行的时间来衡量的。最短作业优先算法总是优先调度要求运行时间最短的作业，把它作为下一次服务的对象。
- 响应比高优先(HRN)：响应比高的作业优先启动。定义响应比为

$$R_p = \frac{\text{作业响应时间}}{\text{作业执行时间}}$$

其中，作业响应时间为作业进入系统后的等候时间与作业的执行时间之和，因此

$$R_p = 1 + \frac{\text{作业等待时间}}{\text{作业执行时间}}$$

- 优先级调度算法：为每个作业确定一个优先数，资源能满足且优先数高的作业优先被选取，当几个作业有相同优先数时，对这些具有相同优先数的作业再按照先来先服务算法进行调度。
- 均衡调度算法：根据作业对资源的要求进行分类，从各类作业中去挑选，尽可能地使得使用不同资源的作业同时执行。

12.2.3　系统开发和运行基础

12.2.3.1　需求分析和设计方法

1. 软件工程

为了消除软件危机，通过认真研究解决软件危机的方法，人们认识到软件工程是使计算机软件走向科学的途径，逐渐形成了软件工程的概念，并开辟了工程学的新兴领域，即软件工程学。

1) 软件工程的 3 个要素

软件工程的 3 个要素如下。

- 方法：完成软件工程项目的技术手段。
- 工具：支持软件的开发、管理、文档生成。
- 过程：过程则是将软件工程的方法和工具综合起来以达到合理、及时地进行计算

机软件开发的目的。过程定义了方法使用的顺序、要求交付的文档资料、为保证质量和协调变化所需要的管理及软件开发各个阶段完成的里程碑。

2) 软件生命周期

软件生命周期是指软件产品从考虑其概念开始到该软件产品交付使用，直至最终退役为止的整个过程。它包括计划阶段、分析阶段、设计阶段、实现阶段、测试阶段和运行维护阶段。

3) 软件开发模型

比较经典的软件开发模型有瀑布模型、快速原型模型、演化模型、增量模型、螺旋模型、喷泉模型等。

4) 软件开发方法

软件开发有以下几种方法。

(1) 结构化软件开发方法(SASD)：采用结构化技术来完成软件开发的各项任务，它把软件生命周期划分成若干阶段，依次地完成每个阶段的任务，它与瀑布模型有很好的结合度，是与其最相适应的软件开发方法。

(2) 面向数据结构的软件开发方法：从目标系统的输入、输出数据结构入手，导出程序框架结构，再补充其他细节，从而得到完整的程序结构图。它有 Jackson 和 Warnier 两种方法。

(3) 面向对象的软件开发方法：随着 OOP(面向对象编程)向 OOD(面向对象设计)和 OOA(面向对象分析)的发展，最终形成面向对象的软件开发方法 OMT(Object Modelling Technique)。这是一种自底向上和自顶向下相结合的方法，而且它以对象建模为基础，从而不仅考虑了输入、输出数据结构，实际上也包含了所有对象的数据结构。

(4) 基于构件化的开发方法：用预先建立的构件和模板，像“搭积木”一样进行建造。

2. 需求分析

(1) 任务：①确定软件系统的功能需求和非功能需求；②分析软件系统的数据要求；③导出系统的逻辑模型；④修正项目开发计划；⑤如有必要，可以开发一个原型。

(2) 主要工作：①需求获取——确定对目标系统的各方面需求。涉及的主要任务是建立获取用户需求的方法框架，并支持和监控需求获取的过程；②需求分析和综合——对问题进行分析，然后在此基础上整合出解决方案；③编写需求规格说明书——对已确定的需求进行文档化描述，该文档通常称为“软件需求规格说明书”；④需求评审——评审需求分析的正确性、完整性和清晰性。

(3) 软件需求规格说明书：软件需求规格说明书是需求分析阶段的最后成果，是软件开发的重要文档之一。其作用有三：①便于用户、开发人员进行理解和交流；②反映出用户问题的结构，可以作为软件开发工作的基础和依据；③作为确认测试和验收的依据。软件需求规格说明书的内容主要包括：概述、数据描述、功能描述、性能描述、参考文献、附录等。

3. 结构化分析方法

结构化分析方法(Structured Analysis，SA)是面向数据流进行需求分析的方法，采用自顶向下、逐层分解，建立系统的处理流程，以数据流图和数据字典为主要工具，建立系统的逻辑模型。SA 方法的分析结果由以下几部分组成：一套分层的数据流图、一本数据词典、



一组小说明。

1) 数据流图

数据流图(Data Flow Diagram，DFD)用来描述数据流从输入到输出的变换流程。它以图形的方式描绘数据在系统中流动和处理的过程，它只反映系统必须完成的逻辑功能，所以是一种功能模型。

DFD 的基本元素如图 12.7 所示。

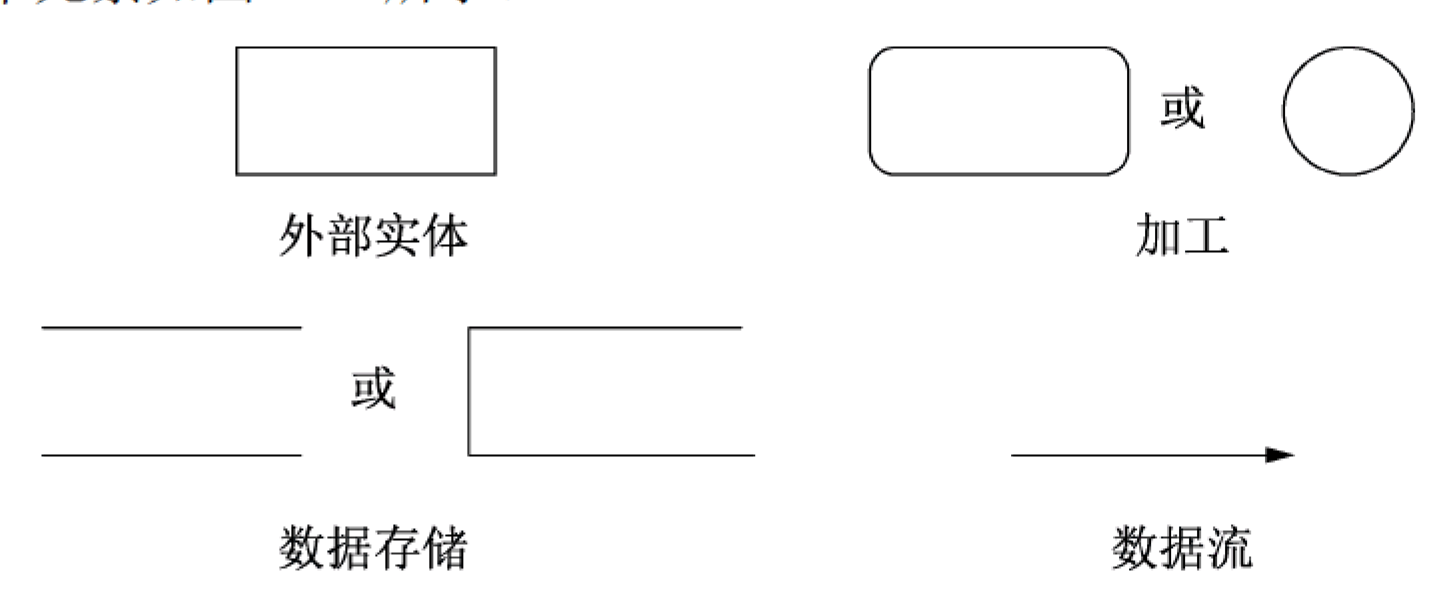


图 12.7　DFD 的基本元素

- 数据流：由一组固定成分的数据组成，表示数据的流向。
- 加工：描述了输入数据流到输出数据流之间的变换，也就是输入数据流经过什么处理后变成了输出数据流。
- 数据存储：用来表示暂时存储的数据，每个数据存储都有一个名字。
- 外部实体：是指存在于软件系统之外的人员或组织。

2) 数据字典

数据流图仅描述了系统的“分解”，而没有对图中各成分进行说明。数据字典就是用来定义数据流图中各个成分的含义的。

数据字典有 4 类条目，包括数据流、数据项、数据存储和基本加工。

3) 加工逻辑的描述

加工逻辑的描述用来说明 DFD 中的数据的加工细节，表达“做什么”，而不是“怎样做”。描述工具有结构化语言、判定表和判定树。

4. 软件设计

从技术角度上看，软件设计可分成体系结构设计、数据设计、接口设计、过程设计 4 方面的工作。从管理角度上看，软件设计分为概要设计、详细设计两个阶段。

1) 软件设计的基本原理

软件设计的基本原理如下。

- 模块化：模块化是指将一个待开发的软件分解成若干小的简单的部分——模块，每个模块可独立地开发、测试，最后组装成完整的程序。
- 抽象化：抽象是一种设计技术，是指抽出事物本质的共同特性而暂不考虑它的细节。
- 信息隐蔽：将每个程序的成分隐蔽或封装在一个单一的设计模块中。定义每一个模块时都应尽可能少地显露其内部的处理，以提高软件的可修改性、可测试性和可移植性。

- 模块独立：模块独立是指每个模块完成一个相对独立的特定子功能，并且与其他模块之间的联系简单。其衡量标准有两个，即模块间的耦合和模块的内聚度。模块独立性强必须做到高内聚、低耦合。

2) 结构化设计方法

结构化设计方法(SD)是一种面向数据流的设计方法，它可以与 SA 方法衔接。

在需求分析阶段，用 SA 方法产生了数据流图。面向数据流的设计能方便地将 DFD 转换成程序结构图。DFD 从系统的输入数据流到系统的输出数据流的一连串连续变换形成了一条信息流。DFD 的信息流大体上可以分为两种类型：一种是变换流，另一种是事务流。

3) 软件详细设计

软件详细设计的任务是为软件结构图中的每一个模块确定实现算法和局部数据结构，用某种选定的表达工具表示算法和数据结构的细节。

结构化程序设计的基本要点如下。

- 采用自顶向下、逐步求精的程序设计方法。
- 使用顺序、选择、重复 3 种基本控制结构构造程序。
- 主程序员组的组织形式。

处理过程设计的关键是用一种合适的表达方法来描述每个模块的执行过程。这种表示方法应该简明、精确，并因此能直接导出用编程语言表示的程序。常用的描述方式有图形、语言和表格 3 类，如传输的框图、各种程序语言和判定表等。

- 程序流程图：程序流程图包括 3 种基本成分：加工步骤，用方框表示；逻辑条件，用菱形表示；控制流，用箭头表示。
- 盒图(NS 图)：在 NS 图中，每个处理步骤用一个盒子表示，盒子可以嵌套。盒子只能从上面进入，从下面走出，除此之外别无其他出入口，所以盒图限制了随意的控制转移，保证了程序的良好结构。
- 形式语言：形式语言是用来描述模块具体算法的非正式而比较灵活的语言。形式语言的优点是接近自然语言，所以易于理解。
- 决策树：决策树是一种图形工具，适合于描述加工中具有多个策略，每个策略和若干条件有关的逻辑功能。
- 决策表：决策表是一种图形工具，呈表形。决策表将比较复杂的决策问题简洁地描述出来。

4) 面向数据结构设计——Jackson 方法

面向数据结构设计是以数据结构作为设计的基础，它根据输入输出数据结构导出程序的结构，适用于规模不大的数据处理系统。Jackson 方法是一种典型的面向数据结构的设计方法。

5) 用户界面设计

用户界面设计是系统与用户之间的接口，也是控制和选择信息输入输出的主要途径。用户界面设计应坚持友好、简便、实用、易于操作的原则。

界面设计包括菜单方式、会话方式、操作提示方式，以及操作权限管理方式等。

5. 面向对象分析与设计

1) 面向对象设计的基本概念

对象：一组属性以及这组属性上的专用操作的封装体，通常由对象名、属性和操作 3 个部分组成。属性表示该对象的状态，用户只能看见对象封装界面上的信息，对象的内部实现对用户是隐蔽的。封装目的是使对象的定义和实现分开。

类：一组具有相同属性和相同操作的对象的集合。一个类中的每个对象都是这个类的一个实例(Instance)。

继承：在某个类的层次关联中不同的类共享属性和操作的一种机制。一个父类可以有多个子类，这些子类都是父类的特例。父类描述了这些子类的公共属性的操作，子类中还可以定义它自己的属性和操作。一个子类只有唯一的一个父类，这种继承称为单一继承。一个子类有多个父类，可以从多个父类中继承特性，这种继承称为多重继承。

消息：对象间通信的手段，一个对象通过向另一对象发送消息来请求其服务。消息通常包括接收对象名、调用的操作名和适当的参数(如有必要)。消息只告诉接收对象需要完成什么操作，并不指示接收者怎样完成操作。消息完全由接收者解释，接收者独立决定采用什么方法来完成所需的操作。

多态性：同一个操作作用于不同的对象可以有不同的解释，产生不同的执行结果。

继承性是面向对象程序设计语言不同于其他语言的主要特点，是否建立了丰富的类库是衡量一个面向对象程序设计语言成熟与否的重要标志之一。

在面向对象的软件工程中，一个组件(Component)包含了一些协作的类的集合。

2) 面向对象分析与设计的基本概念

面向对象方法的基本思想是从现实世界中客观存在的事物出发来构造软件系统。面向对象分析(Object-Oriented Analysis，OOA)的目标是建立待开发软件系统的模型。面向对象设计(Object-Oriented Design，OOD)的目标是定义系统构造蓝图、设计分析模型和实现相应源代码，在目标代码环境中这种源代码可被执行。

统一建模语言(UML)是面向对象软件的标准化建模语言。UML 由 3 个要素构成：UML 的基本构造块、支配这些构造块如何放置在一起的规则和运用于整个语言的一些公共机制。UML 的词汇表包含 3 种构造块：事物、关系和图。事物是对模型中最具代表性的成分的抽象，关系把事物结合在一起，图聚集了相关的事物。

- 事物：包括结构事物、行为事物、分组事物和注释事物。
- 关系：包括依赖、关联、泛化和实现。
- 图：包括类图、对象图、用例图、序列图、协作图、状态图、活动图、构件图和部署图。

12.2.3.2　项目管理基础知识

项目管理的核心内容就是在成本、质量、进度间的平衡。它包括 POIM 四个方面：Plan(计划)、Organize(组织)、Implement(实现)、Measurement(度量)。

1. 项目计划

项目计划的主要内容包括：①估算所需要的人力(通常以人月为单位)、项目持续时间(以

年份或月份为单位)、成本(以元为单位)；②做出进度安排，分配资源，建立项目组织及任用人员(包括人员的地位、作用、职责、规章制度等)，根据规模和工作量估算分配任务；③进行风险分析，包括风险识别、风险估计、风险优化、风险驾驭策略、风险解决和风险监督，这些步骤贯穿在软件工程过程中；④制定质量管理指标；⑤编制预算和成本；⑥准备环境和基础设施等。

2. 质量计划、管理和评估

1) 软件质量度量模型

目前有多种软件质量模型，常用的有以下两种。

- ISO/IEC 9126 软件质量模型。该模型由 3 个层次组成：第一层是质量特性；第二层是质量子特性；第三层是度量指标。
- Mc Call 软件质量模型。该模型从软件产品的运行、修正、转移等 3 个方面确定了 11 个质量特性。它给出了一个 3 层模型框架：第一层是质量特性；第二层是评价准则；第三层是度量指标。

2) 质量管理

质量管理通过制定质量方针、建立质量目标和标准(Target)，并在项目生命周期内持续使用质量计划(Plan)、质量控制(Do)、质量保证(Check)和质量改进(Action)等措施来落实质量方针的执行，确保质量目标的实现，最大限度地使客户满意。

3) 软件质量评审

软件质量评审主要包括设计质量评审和程序质量评审。

3. 进度管理

软件开发项目的进度安排有以下两种方式。

- 系统最终交付日期已经确定，软件开发部门必须在规定期限内完成。
- 系统最终交付日期只确定了大致的年限，最后交付日期由软件开发部门确定。

进度安排的常用图形描述方法有甘特图(Gantt)和计划评审技术图(PERT)。

1) 甘特图

甘特图(Gantt)用水平线段表示任务的工作阶段；线段的起点和终点分别对应着任务的开工时间和完成时间；线段的长度表示完成任务所需的时间。

优点：能清晰地描述每个任务从何时开始到何时结束以及各个任务之间的并行性。

缺点：不能清晰地反映出各任务之间的依赖关系，难以确定整个项目的关键所在，也不能反映计划中有潜力的部分。

2) 计划评审技术图

计划评审技术图(PERT)是一个有向图，图中的有向弧表示任务，它可以标上完成该任务所需的时间；图中的节点表示流入节点的任务的结束，并开始流出节点的任务，这里把节点称为事件。只有当流入该节点的所有任务都结束时，节点所表示的事件才出现，流出节点的任务才可以开始。事件本身不消耗时间和资源，它仅表示某个时间点。每个事件有一个事件号和出现该事件的最早时刻和最迟时刻。每个任务还有一个松弛时间，表示在不影响整个工期的前提下，完成该任务有多少机动余地。松弛时间为 0 的任务构成了完成整个工程的关键路径。



PERT 图不仅给出了每个任务的开始时间、结束时间和完成该任务所需的时间，还给出了任务之间的关系，即哪些任务完成后才能开始另外一些任务，以及如期完成整个工程的关键路径。松弛时间则反映了完成某些任务时可以推迟其开始时间或延长其所需的完成时间。但是 PERT 图不能反映任务之间的并行关系。

4. 文档管理

文档是软件产品的一部分，没有文档的软件就不称其为软件。国家标准《计算机软件产品开发文件编制指南》(GB8567—88)中规定，在一项软件开发过程中，一般来说应该产生 14 种文件。

5. 人员管理

可以按软件项目对软件人员分组，如需求分析组、设计组、编码组、测试组、维护组等，为了控制软件的质量，还可以有质量保证组。

6. 风险管理

风险分析在软件项目管理中具有决定性作用，它是贯穿在软件工程中的一系列风险管理步骤，其中包括：风险识别、风险估计、风险管理策略、风险解决和风险监督。

7. 软件工具与软件开发环境

1) 软件工具

通常可将软件工具分为软件开发工具、软件维护工具和软件管理工具。

2) 软件开发环境

软件开发环境是支持软件产品开发的软件系统，它由工具集和环境集成机制两部分组成。工具集中还应该包含支持软件生命周期各阶段活动以及支持各种开发方法和开发模型的工具，能支持软件开发的全过程。而环境集成机制主要包含数据集成机制、控制集成机制和界面集成机制三方面内容。

8. 能力成熟度模型简介

能力成熟度模型(CMM)用于衡量软件企业的开发管理水平，它可作为软件发包方评估承包方执行能力的参考标准，也可以被软件企业作为软件过程改进工作的参考模型。CMM 模型将软件过程的成熟度分为 5 个等级：初始级、可重复级、已定义级、已管理级和优化级。

12.2.3.3　软件的测试与调试

1. 软件测试的目的

软件测试的目的是尽可能多地发现软件产品(主要是指程序)中的错误和缺陷。成功的测试是发现了至今未发现的错误的测试。

2. 测试过程

一个规范的测试过程通常包括：制订测试计划、编制测试大纲、根据测试大纲设计和生成测试用例、实施测试和生成测试报告。

3. 测试方法

测试的关键是测试用例的设计。软件测试的种类大致可以分为人工测试和动态测试，动态测试方法又根据测试用例的设计方法不同，分为白盒测试和黑盒测试。

1) 白盒测试

白盒测试法需要了解程序内部的结构，测试用例是根据程序的内部逻辑来设计的。白盒测试法主要用于软件的单元测试。

白盒测试的基本原则如下。

- 保证所测模块中每一个独立路径至少执行一次。
- 保证所测模块所有判断的每一个分支至少执行一次。
- 保证所测模块每一个循环都在边界条件和一般条件至少执行一次。
- 验证所有内部数据结构的有效性。

白盒测试法常用的技术是逻辑覆盖，主要的覆盖标准有 6 种，强度由低到高依次是：语句覆盖、判定覆盖、条件覆盖、判定/条件覆盖、条件组合覆盖、路径覆盖。

2) 黑盒测试

黑盒测试是对软件已经实现的功能是否满足需求进行测试和验证。黑盒测试不关心程序内部的逻辑，只是根据程序的功能说明来设计测试用例。黑盒测试法主要用于软件的确认测试。

测试方法有以下几种。

- 等价类划分：把输入数据划分成若干有效等价类和无效等价类，然后设计测试用例覆盖这些等价类。
- 边界值分析：对各种输入、输出范围的边界情况设计测试用例的方法。这是因为程序在处理边界情况时出错的概率比较大。
- 错误猜测：根据经验或直觉推测程序中可能存在的各种错误。
- 因果图：根据输入条件与输出结果之间的因果关系来设计测试用例。

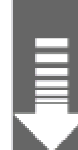
4. 软件测试步骤

(1) 单元测试：单元测试也称模块测试，主要发现编码和详细设计中产生的错误，通常采用白盒测试。该测试放在编码阶段，由程序员自己来完成，检查它是否实现了详细设计说明书中规定的模块功能和算法。单元测试的测试计划是在详细设计阶段完成。

(2) 集成测试：集成测试也称组装测试，是对由各模块组装而成的程序进行测试，主要检查模块间的接口和通信。集成测试主要发现设计阶段产生的错误，通常采用黑盒测试或灰盒测试。集成的方式可分成非渐增式集成和渐增式集成。集成测试的测试计划是在概要设计阶段完成。

(3) 确认测试：检查软件的功能、性能及其他特征是否与用户的需求一致，它是以需求规格说明书(即需求规约)作为依据的测试。确认测试通常采用黑盒测试，其测试计划是在需求分析阶段完成。

(4) 系统测试：把已经过确认的软件纳入实际运行环境中，与其他系统成分组合在一起进行测试。系统测试的主要内容包括恢复测试、安全测试、强度测试、性能测试、可靠性测试、安装测试等。



5. 软件调试

调试是在进行了成功的测试之后才开始的工作，其任务是进一步诊断和改正程序中潜在的错误。调试由两部分组成：确定错误的确切性质和位置、修改程序(设计、编码)。目前常用的调试方法有 5 种：试探法、回溯法、对分查找法、归纳法、演绎法。

12.2.3.4　系统维护

1. 系统维护的内容

系统维护的内容如下。

- 硬件维护应由专职的硬件维护人员来负责，主要有两种类型的维护活动：一种是定期的设备保养性维护，另一种是突发性的故障维护。
- 软件维护主要是根据需求变化或硬件环境的变化对应用程序进行部分或全部的修改。
- 数据维护主要是由数据库管理员来负责，主要负责数据库的安全性和完整性以及进行并发性控制。

2. 软件维护的内容

软件维护的内容包括：正确性维护、适应性维护、完善性维护和预防性维护等。

3. 软件可维护性的质量特性

软件可维护性可以用以下 7 个质量特性来衡量：可理解性、可测试性、可修改性、可靠性、可移植性、可使用性和效率。

12.2.4　标准化和信息化

12.2.4.1　标准化知识

制定标准的目的是获得最佳秩序，促进最佳社会效益。制定标准应遵循的原则是：要从全局利益出发，认真贯彻国家技术经济政策；充分满足使用要求；有利于促进科学技术的发展。

标准化的主要形式有简化、统一化、系列化、通用化及组合化。

1. 标准的代号和编号

1) 国际、国外标准代号及编号

国际、国外标准代号及编号的基本结构为：标准代号+专业类号+顺序号+年代号。

2) 我国标准代号及编号

我国标准代号及编号的基本结构为：标准代号+标准发布顺序号+标准发布年号。

2. 标准的有效期

标准的有效期自标准实施之日起，至标准复审重新确认、修订或废止的时间。ISO 标准每 5 年复审一次，平均标龄为 4.92 年。我国在 1988 年发布的《中华人民共和国标准化法实施条例》中规定，国家标准实施 5 年内要进行复审，即国家标准的有效期一般为 5 年。

12.2.4.2 知识产权

1. 知识产权的概念

知识产权又称为智慧财产权，是指人们通过自己的智力活动创造的成果以及经营管理活动中的经验、知识而依法所享有的权利。传统的知识产权可分为工业产权和著作权(版权)两类。

工业产权包括专利、实用新型、工业品外观设计、商标、服务标记、厂商名称、产地标记或原产地名称、制止不正当竞争等项内容。此外，商业秘密、微生物技术、遗传基因技术等也属于工业产权保护的对象。

著作权(又称为版权)是指作者对其创作的作品享有的人身权和财产权。它包括发表权、署名权、修改权和保护作品完整权、复制权、发行权、出租权、展览权、表演权、放映权、广播权、信息网络传播权、摄制权、改编权、翻译权、汇编权，以及应当由著作权人享有的其他权利。著作权的保护对象包括文学、科学和艺术领域内的一切作品。

2. 计算机软件著作权的主体与客体

计算机软件著作权的主体是指享有著作权的人，包括公民、法人和其他组织。

计算机软件的客体是指著作权法保护的计算机软件著作权的范围，根据《著作权法》第三条和《计算机软件保护条例》第二条的规定，著作权法保护的是计算机程序及其有关文档。

3. 计算机软件著作权的权利

1) 计算机软件的著作人身权

计算机软件主要有两种权利：人身权(精神权利)和财产权(经济权利)。软件著作人还享有发表权和开发者身份权。

发表权是指是否公布软件作品的权利。开发者身份权又称为署名权，是指软件作者在作品中署自己名字的权利。

2) 计算机软件的著作财产权

计算机软件的著作财产权是指能够给著作权人带来经济利益的权利，通常是指由软件著作权人控制和支配，并能够为权利人带来一定经济效益的权利。其主要内容有：使用权、复制权、修改权、发行权、翻译权、注释权、信息网络传播权、出租权、使用许可权和获得报酬权、转让权等。

4. 计算机软件著作权的保护期

计算机软件著作权自软件开发完成之日起，保护期为50年。保护期满，除开发者身份权外，其他权利终止。计算机软件著作权人的单位终止和计算机软件著作权人的公民死亡且无合法继承人时，除开发者身份权外的其他权利进入公有领域。

5. 计算机软件著作权的归属

1) 软件著作权归属的基本原则

我国《著作权法》规定著作权属于作者。《计算机软件保护条例》规定，软件著作权属于软件开发者。



2) 职务开发软件著作权的归属

当公民作为某单位的雇员时，如其开发的软件属于执行本职工作的结果，则软件著作权应当归单位享有。若开发的软件不是执行本职工作的结果，其著作权不属于单位享有；如果该雇员主要使用了单位的设备，按照《计算机软件保护条例》第十三条第三款规定，不能属于该雇员所有。

3) 合作开发软件著作权的归属

由两个或两个以上的公民、法人或其他组织订立协议，共同开发完成的软件属于合作开发的软件。其著作权的归属一般是共同享有，合作开发者不能单独行使转让权。如果有软件著作权的协议，则按照协议确定软件著作权的归属。

4) 委托开发的软件著作权的归属

受委托创作的作品，著作权的归属由委托人和受托人通过合同约定。合同未作明确约定或者没有订立合同的，著作权属于受托人。

5) 接受任务开发的软件著作权的归属

接受任务开发的软件著作权归属在合同中明确约定的，按照合同约定实行。未明确约定的，著作权属于实际完成软件开发的单位。

6) 计算机软件著作权主体变更后软件著作权的归属

因主体变更引起的变化有以下几种。

- 公民继承的软件权利归属：合法继承人享有除署名权外的其他权利。
- 单位变更后软件权利归属：由承受其权利义务的法人或者其他组织享有；没有承受其权利义务的法人或者其他组织的，由国家享有。
- 权利转让后的软件著作权归属：权利转让根据签订的合同规定各方的权利。
- 司法判决、裁定引起的软件著作权归属问题：根据法律的判决来执行。
- 保护期届满权利丧失。

6. 软件著作权侵权的法律责任

需要承担民事责任的侵权行为有：未经软件著作权人的许可发表或登记其软件的；将他人的软件当作自己的软件发表或登记的；未经合作者许可，将与他人合作开发的软件当作自己独立完成的作品发表或者登记的；在他人开发的软件上署名或者更改他人开发的软件上的署名的；未经软件著作权人或者其合法受让者的许可，修改或翻译其软件的；其他侵犯软件著作权的行为。

需要承担行政责任的侵权行为有：复制或部分复制著作权人的软件的；向公众发行、出租著作权人的软件的；故意避开或者破坏著作权人为保护其软件而采取的技术措施的；故意删除或者改变软件权利管理电子信息的；许可他人行使或者转让著作权人的软件著作权的。

侵权行为触犯法律的，侵权者承担相应的刑事责任。

7. 计算机软件的商业秘密权

我国《反不正当竞争法》中商业秘密被定义为“不为公众所熟悉的、能为权利人带来经济效益、具有实用性并经权利人采取保密措施的技术信息和经营信息”，经营秘密和技术秘密是商业秘密的基本内容。

根据我国《反不正当竞争法》第十条的规定，侵犯计算机软件商业秘密的具体表现形式主要有以下几种。

(1) 以盗窃、利诱、胁迫或以其他不正当手段获取权利人的计算机软件商业秘密。

(2) 披露、使用或允许他人使用以不正当手段获取权利人的计算机软件商业秘密。

(3) 违反约定或违反权利人有关保守商业秘密的要求，披露、使用或允许他人使用其掌握的计算机软件商业秘密的行为。

(4) 第三方在明知前述违法行为的情况下，仍然从侵权人那里获取或使用他人计算机软件商业秘密的行为。该行为属于间接侵权。

8. 专利权

发明创造是产生专利权的基础。发明创造是指发明、实用新型和外观设计，是我国专利法主要保护的对象。《中华人民共和国专利法实施细则》第二条第一款规定：“专利法所称的发明，是指对产品、方法或者其改进所提出的新的技术方案。” 一项发明或者实用新型获得专利的实质条件为新颖性、创造性和实用性。

专利申请采用书面形式，一项专利申请文件只能申请一项专利。发明或者实用新型的专利申请文件包括请求书、说明书、说明书摘要、权利要求书。外观设计专利申请文件包括请求书、图片或照片。两个或两个以上的人就同样的发明创造申请专利的，专利权授予最先申请人。专利局收到发明专利申请后，一个必要程序是初步审查，经初步审查认为符合本法要求的，自申请日起满 18 个月，即行公布。专利局可根据申请人的请求，早日公布其申请。自申请日起 3 年内，专利局可根据申请人随时提出的请求，对其申请进行实质审查。实质审查是依法审查专利的新颖性、创造性和实用性。

根据我国专利法的规定，发明专利的保护期限为 20 年，实用新型和外观设计专利为 10 年。

12.3 真题详解

试题 1 (2017 年下半年试题 1)

在程序的执行过程中，Cache 与主存的地址映射是由__(1)__完成的。

(1) A. 操作系统　　B. 程序员调度

C. 硬件自动　　D. 用户软件

参考答案：(1)C。

要点解析：Cache 地址的映射是由硬件实现的，以达到快速访问的目的，对用户和程序员是透明的。

试题 2 (2017 年下半年试题 2)

某四级指令流水线分别完成取指、取数、运算、保存结果四步操作。若完成上述操作的时间依次为 8ns、9ns、4ns、8ns，则该流水线的操作周期应至少为__(2)__ns。

(2) A. 4　　B. 8　　C. 9　　D. 33

参考答案：(2)C。

要点解析：流水线的操作周期取决于基本操作时间最长的一个。



试题 3　(2017 年下半年试题 3)

内存按字节编址。若用存储容量为 32K×8bit 的存储器芯片构成地址从 A0000H 到 DFFFFH 的内存，则至少需要__(3)__片芯片。

(3)　A. 4　　B. 8　　C. 16　　D. 32

参考答案：(3)B。

要点解析：(DFFFFH−A0000H+1)/32=8(片)。

试题 4　(2017 年下半年试题 4)

计算机系统的主存主要是由__(4)__构成的。

(4)　A. DRAM　　B. SRAM　　C. Cache　　D. EEPROM

参考答案：(4)A。

要点解析：DRAM 动态随机存取存储器，最为常见的系统内存。为了保持数据，DRAM 必须周期性刷新。

试题 5　(2017 年下半年试题 5)

计算机运行过程中，CPU 需要与外设进行数据交换。采用__(5)__控制技术时，CPU 与外设可并行工作。

(5)　A. 程序查询方式和中断方式
　　B. 中断方式和 DMA 方式
　　C. 程序查询方式和 DMA 方式
　　D. 程序查询方式、中断方式和 DMA 方式

参考答案：(5)B。

要点解析：程序查询方式中 CPU 通过执行程序查询外设的状态，判断外设是否准备好进行数据传送，由 CPU 全程控制，因此不能实现与外设的并行工作。DMA(直接存储器存取)采用专门的控制器来控制内存和外设之间的数据交流，无须 CPU 介入，大大提高了 CPU 的工作效率。中断方式在外设做好数据传送之前，CPU 可以做自己的事情，发出中断请求以后，CPU 响应才会控制其数据传输过程，一定程度上能实现 CPU 和外设的并行。

试题 6　(2017 年下半年试题 6)

李某购买了一张有注册商标的应用软件光盘，则李某享有__(6)__。

(6)　A. 注册商标专用权　　B. 该光盘的所有权
　　C. 该软件的著作权　　D. 该软件的所有权

参考答案：(6)B。

要点解析：购买软件仅拥有该软件的使用权。

试题 7　(2017 年下半年试题 7 和试题 8)

某软件项目的活动图如图 12.8 所示，其中顶点表示项目里程碑，连接顶点的边表示包含的活动，边上的数字表示活动的持续时间(天)。完成该项目的最少时间为__(7)__。

由于某种原因，现在需要同一个开发人员完成 BC 和 BD，到完成该项目如最少时间为__(8)__天。

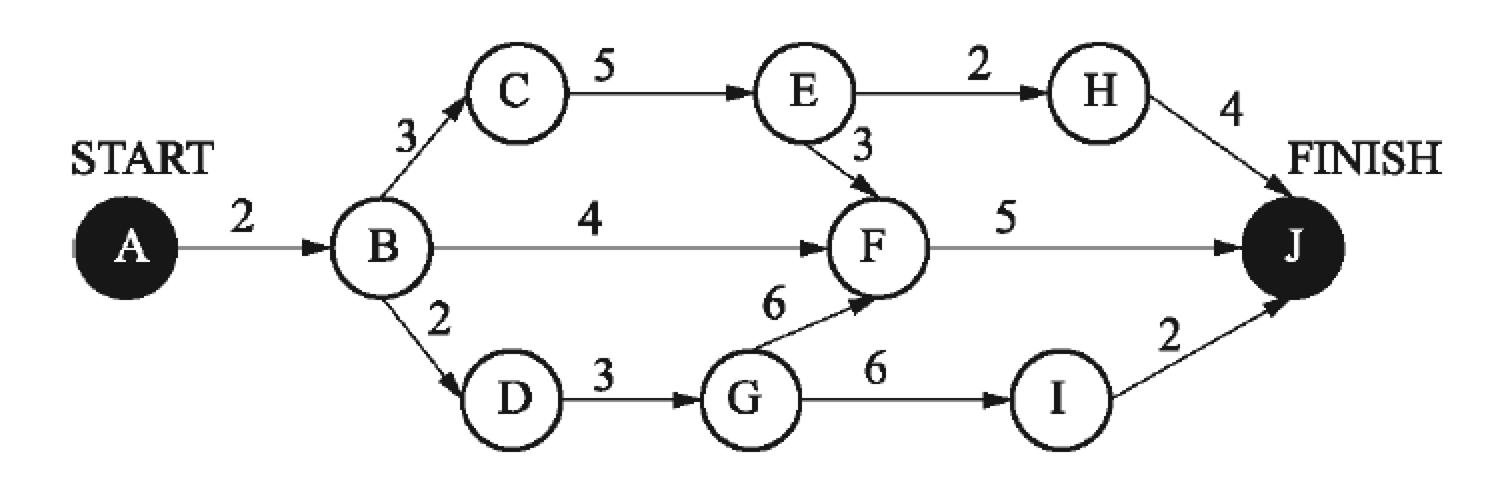


图 12.8 某软件项目的活动图

(7) A. 11　　B. 18　　C. 20　　D. 21

(8) A. 11　　B. 18　　C. 20　　D. 21

参考答案：(7)B；(8)C。

要点解析：本题的关键路径可知为 ABCEFJ 和 ABDGFJ，都是 18。

若由同一个开发人员完成 BC 和 BD，两个任务不可能并行工作，故存在一个先后问题。若先完成 BD，则相当于 BC 用时 3+2=5(天)，总工期为 20 天；若先完成 BC，则 BD 用时 2+3=5(天)，总工期为 21 天。所以至少需要 20 天。

试题 8 (2017 年下半年试题 9)

以下关于程序设计语言的叙述中，错误的是__(9)__。

(9) A. 脚本语言中不使用变量和函数　　B. 标记语言常用于描述格式化和链接

C. 脚本语言采用解释方式实现　　D. 编译型语言的执行效率更高

参考答案：(9)A。

要点解析：脚本语言如 JavaScript 可以使用变量和函数。

试题 9 (2017 年下半年试题 10)

在基于 Web 的电子商务应用中，访问存储于数据库中的业务对象的常用方式之一是__(10)__。

(10) A. JDBC　　B. XML　　C. CGI　　D. COM

参考答案：(10)A。

要点解析：数据库链接(JDBC)由一组用 Java 编程语言编写的类和接口组成，它提供了一个标准的 API。

试题 10 (2017 年上半年试题 1)

CPU 执行算术运算或者逻辑运算时，常将源操作数和结果暂存在__(1)__中。

(1) A. 程序计数器(PC)　　B. 累加器(AC)

C. 指令寄存器(IR)　　D. 地址寄存器(AR)

参考答案：(1)B。

要点解析：累加寄存器(AC)简称为累加器，其功能是：当运算器的算术逻辑单元(ALU)执行算术或逻辑运算时，为 ALU 提供一个工作区。累加寄存器暂存 ALU 运算中的结果信息。

试题 11 (2017 年上半年试题 2)

某系统由图 12.9 所示的冗余部件构成。若每个部件的千小时可靠度都为 R，则该系统



的千小时可靠度为___(2)___。

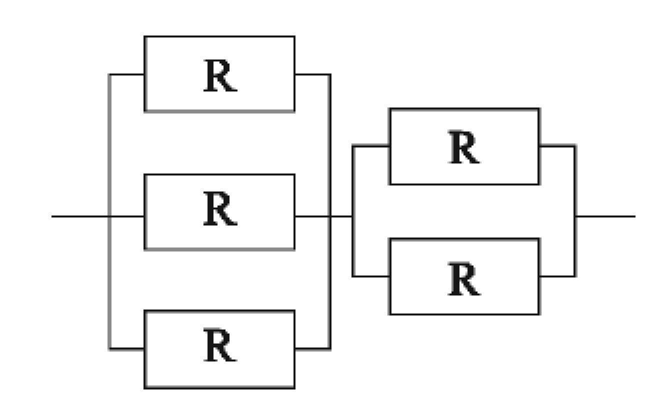


图 12.9 冗余部件

(2) A. $(1-R^3)(1-R^2)$　　B. $(1-(1-R)^3)(1-(1-R)^2)$
　　C. $(1-R^3)+(1-R^2)$　　D. $(1-(1-R)^3)+(1-(1-R)^2)$

参考答案：(2)B。

要点解析：第一个并联可靠度为 $1-(1-R)^3$，二个并联可靠度为 $1-(1-R)^2$，所以该系统串联的可靠度为 $(1-(1-R)^3)(1-(1-R)^2)$。

试题 12 (2017 年上半年试题 4 和试题 5)

某软件项目的活动图如图 12.10 所示，其中顶点表示项目里程碑，连接顶点的边表示包含的活动，边上的数字表示活动的持续时间(天)，则完成该项目的最少时间为___(4)___天。活动 BD 和 HK 最早可以从第___(5)___天开始。(活动 AB、AE 和 AC 最早从第 1 天开始)

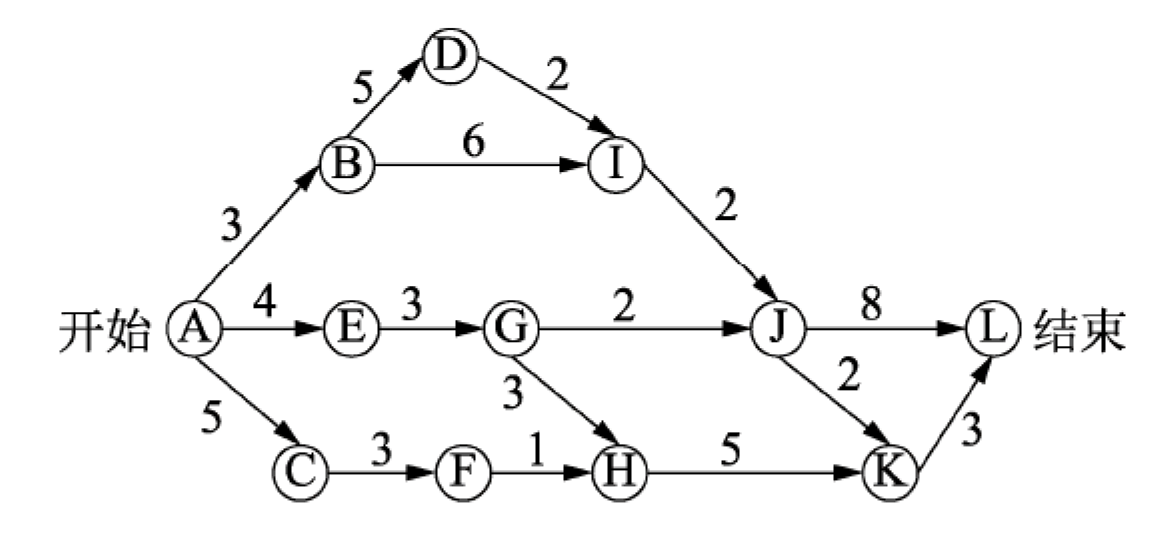


图 12.10 某软件项目的活动图

(4) A. 17　　B. 18　　C. 19　　D. 20
(5) A. 3 和 10　　B. 4 和 11　　C. 3 和 9　　D. 4 和 10

参考答案：(4)D；(5)B。

要点解析：本题考查的是 PERT 图。要求完成该项目的最少时间即为求该项目的关键路径，关键路径是所需时间最长的任务流——ABDIJL，20 天。

活动 BD 需在活动 AB 完成后才能开始进行，而活动 AB 需要 3 天的时间，故活动 BD 可在第 4 天的时候开展。而活动 HK 最早开始需要 AEGH(10 天)和 ACFH(9 天)均完成后才能开始，故其应在第 11 天开展。

试题 13 (2017 年上半年试题 7)

使用图像扫描仪以 300DPI 的分辨率扫描一幅 3×4 英寸的图片，可以得到___(7)___像素的数字图像。

(7) A. 300×300　　B. 300×400　　C. 900×4　　D. 900×1200

参考答案：(7)D。

要点解析：该图片像素为(3×300)×(4×300)。

试题 14　(2017 年上半年试题 8)

某计算机系统页面大小为 4K，进程的页面变换表如表 12.2 所示。若进程的逻辑地址为 2D16H。该地址经过变换后，其物理地址应为__(8)__。

表 12.2　进程的页面变换表

页　号	物理块号
0	1
1	3
2	4
3	6

(8)　A. 2048H　　B. 4096H　　C. 4D16H　　D. 6D16H

参考答案：(8)C。

要点解析：页面大小 $4K=2^{12}$B。逻辑地址 2D16H=0010110100010110=页号(2)+页内偏移量(即 D16)。根据表 12.2 可知页号 2 对应物理块号 4，则其物理地址=物理块号(4)+偏移量(D16)即 4D16。

试题 15　(2017 年上半年试题 9)

根据我国商标法，下列商品中必须使用注册商标的是__(9)__。

(9)　A. 医疗仪器　　B. 墙壁涂料　　C. 无糖食品　　D. 烟草制品

参考答案：(9)D。

要点解析：目前根据我国法律法规的规定必须使用注册商标的是烟草类商品。《烟草专卖法》(1991 年 6 月 29 日通过，1992 年 1 月 1 日施行)第二十条规定："卷烟、雪茄烟和有包装的烟丝必须申请商标注册，未经核准注册的，不得生产、销售。禁止生产、销售假冒他人注册商标的烟草制品。"

试题 16　(2017 年上半年试题 10)

甲、乙两人在同一天就同样的发明创造提交了专利申请，专利局将分别向各申请人通报有关情况，并提出多种可能采用的解决办法，以下说法中，不可能采用的是__(10)__。

(10) A. 甲、乙作为共同申请人
　　B. 甲或乙一方放弃权利并从另一方得到适当的补偿
　　C. 甲、乙都不授予专利权
　　D. 甲、乙都授予专利权

参考答案：(10)D。

要点解析：专利权谁先申请谁拥有，同时申请则协商归属，但不能够同时驳回双方的专利申请。按照专利法的基本原则，对于同一个发明只能授予一个专利权。

试题 17　(2016 年下半年试题 1)

在程序运行过程中，CPU 需要将指令从内存中取出并加以分析和执行。CPU 依据__(1)__来区分在内存中以二进制编码形式存放的指令和数据。

(1)　A. 指令周期的不同阶段　　B. 指令和数据的寻址方式



C. 指令操作码的译码结果　　　　D. 指令和数据所在的存储单元

参考答案：(1)A。

要点分析：冯·诺依曼体系的计算机中指令和数据均以二进制的形式存放在存储器中，CPU 区分它们的方式是依据指令周期的不同阶段。

试题 18 (2016 年下半年试题 2)

计算机在一个指令周期的过程中，为从内存读取指令操作码，首先要将<u>　(2)　</u>的内容送到地址总线上。

(2) A. 指令寄存器(IR)　　　　B. 通用寄存器(GR)
C. 程序计数器(PC)　　　　D. 状态寄存器(PSW)

参考答案：(2)C。

要点解析：程序计数器(PC)用于存放下一指令的地址。计算机执行程序时，在一个指令周期中，要从内存读取指令操作码，首先需要将 PC 的内容送到地址总线上。

试题 19 (2016 年下半年试题 3)

设 16 位浮点数，其中阶符 1 位、阶码值 6 位、数符 1 位、尾数 8 位。若阶码用移码表示，尾数用补码表示，则该浮点数所能表示的数值范围是<u>　(3)　</u>。

(3) A. -2^{64}～$(1-2^{-8})2^{64}$　　　　B. -2^{63}～$(1-2^{-8})2^{63}$
C. $-(1-2^{-8})2^{64}$～$(1-2^{-8})2^{64}$　　　　D. $-(1-2^{-8})2^{63}$～$(1-2^{-8})2^{63}$

参考答案：(3)B。

要点解析：浮点数的结构：尾数部分(定点小数)阶码部分(定点整数)。

9 位补码表示定点小数范围：-1～$+(1-2^{-8})$。

也就是：-1～$+0.11111111$。

非零最小正数：00…0,0.10…0；(2^{-64}) (2^{-1})。

最大正数：11…1,0.11…1；$(2^{63})(1-2^{-8})$。

绝对值最小负数：00…0,1.011…1；$(2^{-64})[-(2^{-1}+2^{-8})]$。

绝对值最大负数：11…1，1.00…0；$(2^{63})(-1)$。

故该浮点数能表示的数值范围是：-2^{63}～$(1-2^{-8})2^{63}$。

试题 20 (2016 年下半年试题 4)

已知数据信息为 16 位，最少应附加<u>　(4)　</u>位校验位，以实现海明码纠错。

(4) A. 3　　　　B. 4　　　　C. 5　　　　D. 6

参考答案：(4)C。

要点解析：海明码是利用奇偶性来检错和校验的方法，其构成方法是在数据位之间插入 r 个校验位来扩大码距，从而实现纠错。N 表示添加了校验码位后整个传输信息的二进制位数，用 K 代表其中有效信息位数，r 表示添加的校验码位数，它们之间的关系应满足：$N=K+r\leq 2^r-1$。题中有效信息位为 16，计算得出最小应添加 5 位校验位。

试题 21 (2016 年下半年试题 5)

将一条指令的执行过程分解为取指、分析和执行三步，按照流水方式执行，若取指时间 $t_{取指}=4\Delta t$、分析时间 $t_{分析}=2\Delta t$，执行时间 $t_{执行}=3\Delta t$，则执行完 100 条指令，需要的时间为<u>　(5)　</u>Δt。

(5) A. 200　　B. 300　　C. 400　　D. 405

参考答案：(5)D。

要点解析：流水线技术执行过程中，前后连续的几个操作可以依次进入，在这个站间重叠执行。执行完 100 条指令的时间为：$(4+2+3)\Delta t+(100-1)\times 4\Delta t=405\Delta t$。

试题 22　(2016 年下半年试题 6)

在敏捷过程的开发方法中，__(6)__使用了迭代的方法，其中，把每段时间(30 天)一次的迭代称为一个“冲刺”，并按需求的优先级别来实现产品，多个自组织和自治的小组并行地递增实现产品。

(6) A. 极限编程 XP　　B. 水晶法

C. 并列争球法　　D. 自适应软件开发

参考答案：(6)C。

要点解析：敏捷开发是针对传统的瀑布开发模式的弊端而产生的一种新的开发模式，目标是提高开发效率和响应能力。常用的开发方法就是极限编程 XP、水晶法、并列争球法、自适应软件开发这四种。极限编程 XP：激发软件人员创造性，管理负担最小。水晶法：每个项目都需要不同策略、约定和方法论。并列争球法：迭代，冲刺，多个自组织的小组并行地递增实现产品。自适应软件开发：使命作为指导，人员协作，团队组织设立项目的目标。

试题 23　(2016 年下半年试题 7 和试题 8)

某软件项目的活动图如图 12.11 所示，其中顶点表示项目里程碑，连接顶点的边表示包含的活动，边上的数字表示相应活动的持续时间(天)，则完成该项目的最少时间为__(7)__天。活动 BC 和 BF 最多可以晚开始__(8)__天而不会影响整个项目的进度。

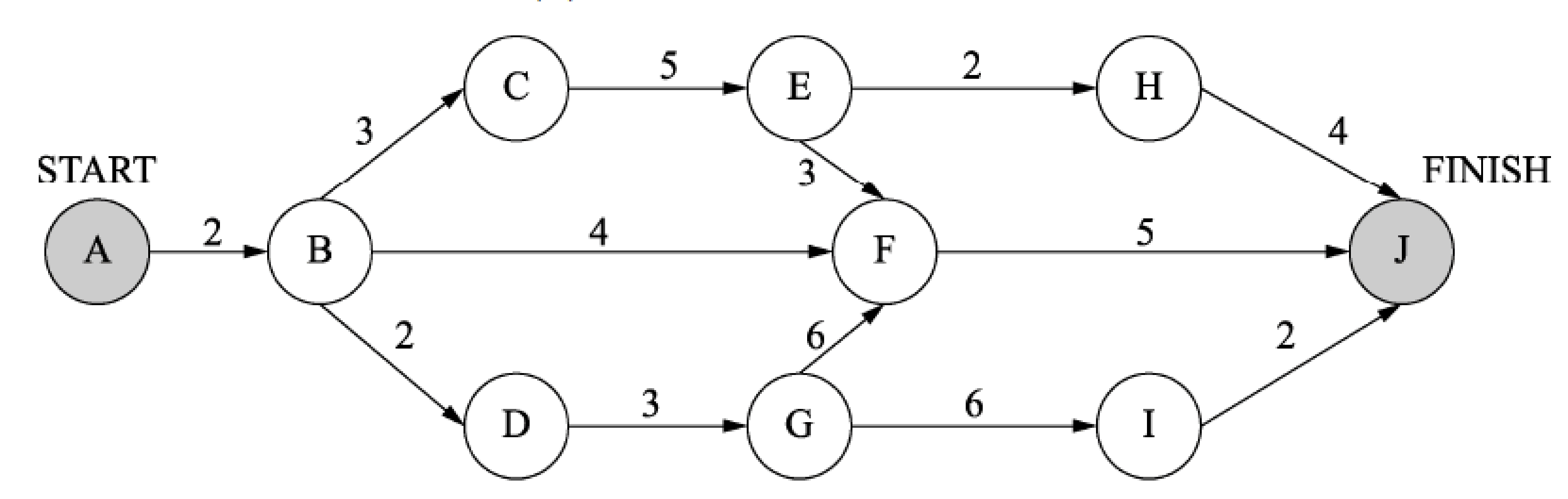


图 12.11　某软件项目的活动图

(7) A. 11　　B. 15　　C. 16　　D. 18

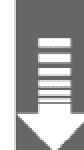
(8) A. 0 和 7　　B. 0 和 11　　C. 2 和 7　　D. 2 和 11

参考答案：(7)D；(8)A。

要点解析：在 PERT 图中，从 start 到 finish 最长的路径就是关键路径，也是完成该项目的最少时间。分析该活动图可知，关键路径为 ABCEFJ 和 ABDGFJ，均为 18 天。BC 所在的路径就是关键路径，松弛时间为 0；BF 所在的路径最长时间为 11，则松弛时间为 18−11=7(天)，故 BF 可以晚开始 7 天。

试题 24　(2016 年下半年试题 9)

假设系统有 n 个进程共享资源 R，且资源 R 的可用数为 3，其中 $n\geq 3$，若采用 PV 操作，



则信号量 S 的取值范围应为 (9) 。

(9) A. $-1\sim n-1$　　B. $-3\sim3$

C. $-(n-3)\sim3$　　D. $-(n-1)\sim1$

参考答案：(9)C。

要点解析：资源 R 的可用数为 3，则信号量的初始值为 3，负数表示所缺资源数，共有 n 个进程，所缺资源数最多为 $n-3$(亦可理解为等待的进程数)，故信号量 S 的取值范围为：$-(n-3)\sim3$。

试题 25 (2016 年下半年试题 10)

甲、乙两厂生产的产品类似，且产品都拟使用“B”商标。两厂于同一天向商标局申请商标注册，且申请注册前两厂均未使用“B”商标。此情形下， (10) 能核准注册。

(10) A. 甲厂　　B. 由甲、乙厂抽签确定的厂

C. 乙厂　　D. 甲、乙两厂

参考答案：(10)B。

要点解析：《商标法实施条例》第十九条：

两个或者两个以上的申请人，在同一种商品或者类似商品上，分别以相同或者近似的商标在同一天申请注册的，各申请人应当自收到商标局通知之日起 30 日内提交其申请注册前在先使用该商标的证据。同日使用或者均未使用的，各申请人可以自收到商标局通知之日起 30 日内自行协商，并将书面协议报送商标局；不愿协商或者协商不成的，商标局通知各申请人以抽签的方式确定一个申请人，驳回其他人的注册申请。商标局已经通知但申请人未参加抽签的，视为放弃申请，商标局应当书面通知未参加抽签的申请人。

试题 26 (2016 年上半年试题 1)

内存按字节编址，从 A1000H 到 B13FFH 的区域的存储容量为 (1) KB。

(1) A. 32　　B. 34　　C. 65　　D. 67

参考答案：(1)C。

要点解析：从 A1000H 到 B13FFH 的存储单元数为(B13FFH−A1000H)+1=10400H，存储容量为 10400H/1024=65KB。

试题 27 (2016 年上半年试题 2)

以下关于总线的叙述中，不正确的是 (2) 。

(2) A. 并行总线适合近距离高速数据传输

B. 串行总线适合长距离数据传输

C. 单总线结构在一个总线上适应不同种类的设备，设计简单且性能很高

D. 专用总线在设计上可以与连接设备实现最佳匹配

参考答案：(2)C。

要点解析：在单总线结构中，CPU 与主存之间、CPU 与 I/O 设备之间、I/O 设备与主存之间、各种设备之间都通过系统总线交换信息。单总线结构的优点是控制简单方便，扩充方便。但由于所有设备部件均挂在单一总线上，使这种结构只能分时工作，即同一时刻只能在两个设备之间传送数据，这就使系统总体数据传输的效率和速度受到限制，这是单总

线结构的主要缺点。

试题 28 (2016 年上半年试题 3)

某软件公司参与开发管理系统软件的程序员张某，辞职到另一公司任职，于是该项目负责人将该管理系统软件上开发者的署名更改为李某(接张某工作)。该项目负责人的行为__(3)__。

(3) A. 侵犯了张某开发者身份权(署名权)
B. 不构成侵权，因为程序员张某不是软件著作权人
C. 只是行使管理者的权利，不构成侵权
D. 不构成侵权，因为程序员张某现已不是项目组成员

参考答案：(3)A。

要点解析：张某参加某软件公司开发管理系统软件的工作，属于职务行为，该管理系统软件的著作权归属公司所有，但根据《著作权法》张某拥有该管理系统软件的署名权。而该项目负责人将作为软件系统开发者之一的张某的署名更改为他人，根据《计算机软件保护条例》第 23 条第 4 款的规定，项目负责人的行为侵犯了张某的开发者身份权及署名权。

试题 29 (2016 年上半年试题 4)

以下媒体文件格式中__(4)__是视频文件格式。

(4) A. WAV B. BMP C. MP3 D. MOV

参考答案：(4)D。

要点解析：WAV 为微软公司(Microsoft)开发的一种声音文件格式。

BMP(全称 Bitmap)是 Windows 操作系统中的标准图像文件格式。

MP3 是一种音频压缩技术。

MOV 是 QuickTime 影片格式，它是 Apple 公司开发的一种音频、视频文件格式，用于存储常用数字媒体类型。

试题 30 (2016 年上半年试题 5)

使用 150DPI 的扫描分辨率扫描一幅 3×4 英寸的彩色照片，得到原始的 24 位真彩色图像的数据量是__(5)__Byte。

(5) A. 1800 B. 90000 C. 270000 D. 810000

参考答案：(5)D。

要点解析：150DPI 的扫描分辨率表示每英寸的像素为 150 个，所以数据量为 $3\times150\times4\times150\times24/8=810000$B。

试题 31 (2016 年上半年试题 6)

以下关于脚本语言的叙述中，正确的是__(6)__。

(6) A. 脚本语言是通用的程序设计语言
B. 脚本语言更适合应用在系统级程序开发中
C. 脚本语言主要采用解释方式实现
D. 脚本语言中不能定义函数和调用函数

参考答案：(6)C。



要点解析：脚本语言是为了缩短传统的编写-编译-链接-运行(edit-compile-link-run)过程而创建的计算机编程语言。脚本语言是一种解释性的语言，例如 Python、Javascript、ActionScript 等，它不像 C\C++等可以编译成二进制代码，以可执行文件的形式存在。脚本语言不需要编译，可以直接用，由解释器来负责解释。

试题 32　(2016 年上半年试题 7 和试题 8)

在结构化分析中，用数据流图描述 (7) 。当采用数据流图对一个图书馆管理系统进行分析时， (8) 是一个外部实体。

(7) A. 数据对象之间的关系，用于对数据建模
B. 数据在系统中如何被传送或变换，以及如何对数据流进行变换的功能或子功能，用于对功能建模
C. 系统对外部事件如何响应，如何动作，用于对行为建模
D. 数据流图中的各个组成部分

(8) A. 读者　B. 图书　C. 借书证　D. 借阅

参考答案：(7)B；(8)A。

要点解析：数据流图(Data Flow Diagram，DFD)从数据传递和加工角度，以图形方式来表达系统的逻辑功能、数据在系统内部的逻辑流向和逻辑变换过程，是结构化系统分析方法的主要表达工具及用于表示软件模型的一种图示方法。外部实体是指独立于系统而存在的，但又和系统有联系的实体，它表示数据的外部来源和最后去向。显然，读者是图书馆管理系统的一个外部实体。

试题 33　(2016 年上半年试题 9)

当用户通过键盘或鼠标进入某应用系统时，通常最先获得键盘或鼠标输入信息的是 (9) 。

(9) A. 命令解释　B. 中断处理　C. 用户登录　D. 系统调用

参考答案：(9)B。

要点解析：用键盘当作输入设备，每当用户按下或释放某一个键时，会产生一个中断，该中断激活键盘驱动程序 KEYBOARD.DRV 来对键盘中断进行处理。

试题 34　(2016 年上半年试题 10)

在 Windows 操作系统中，当用户双击“IMG_20160122_103. jpg”文件名时，系统会自动通过建立的 (10) 来决定使用什么程序打开该图像文件。

(10) A. 文件　B. 文件关联　C. 文件目录　D. 临时文件

参考答案：(10)B。

要点解析：当用户双击一个文件名时，Windows 系统通过建立的文件关联来决定使用什么程序打开该文件。如果系统建立了“记事本”程序打开扩展名为.TXT 的文件关联，那么当用户双击*.TXT 文件时，Windows 先执行“记事本”程序，然后打开该文本文件。

试题 35　(2015 年下半年试题 1)

CPU 是在 (1) 结束时响应 DMA 请求的。

(1) A. 一条指令执行　B. 一段程序　C. 一个时钟周期　D. 一个总线周期

参考答案：(1)D。

要点解析：外设向 DMA 控制器(DMAC)提出 DMA 传送的请求；然后 DMA 控制器向 CPU 提出请求；CPU 在完成当前的总线周期后立即对此请求做出相应。总线周期通常指的是 CPU 完成一次访问存储器或 I/O 端口操作所需要的时间。

试题 36 (2015 年下半年试题 2)

虚拟存储体系由__(2)__两级存储器构成。

(2) A. 主存-辅存 B. 寄存器-Cache C. 寄存器-主存 D. Cache-主存

参考答案：(2)A。

要点解析：虚拟存储器采用主存-辅存结构。程序(数据)被分成很多小块，全部存储在辅存。运行时，需要把要用到的块先调入主存，并把马上要用到的块从主存调入高速缓存。

试题 37 (2015 年下半年试题 3)

在机器指令的地址字段中，直接指出操作数本身的寻址方式称为__(3)__。

(3) A. 隐含寻址 B. 寄存器寻址 C. 立即寻址 D. 直接寻址

参考答案：(3)C。

要点解析：隐含寻址：这种类型的指令，不是明显地给出操作数的地址，而是在指令中隐含着操作数的地址。

寄存器寻址：当操作数不放在内存中，而是放在 CPU 的通用寄存器中时，可采用寄存器寻址方式。显然，此时指令中给出的操作数地址不是内存的地址单元号，而是通用寄存器的编号。

立即寻址：指令的地址字段指出的不是操作数的地址，而是操作数本身。立即寻址方式的特点是指令执行时间很短，因为它不需要访问内存取数，从而节省了访问内存的时间。

直接寻址：是一种基本的寻址方法，其特点是在指令格式的地址的字段中直接指出操作数在内存的地址。由于操作数的地址直接给出而不需要经过某种变换，所以称这种寻址方式为直接寻址方式。

试题 38 (2015 年下半年试题 4)

内存按字节编址从 B3000H 到 DABFFH 的区域其存储容量为__(4)__。

(4) A.123KB B.159KB C.163KB D.194KB

参考答案：(4)B。

要点解析：存储地址从 B3000H 到 DABFFH 共有(DABFFH−B3000H+1=27C00H=159K)个存储单元，由于内存地址按字节编址，所以存储容量为 159KB。

试题 39 (2015 年下半年试题 5)

以下关于软件项目管理中人员管理的叙述，正确的是__(5)__。

(5) A. 项目组成员的工作风格也应该作为组织团队时要考虑的一个要素
B. 鼓励团队的每个成员充分地参与开发过程的所有阶段
C. 仅根据开发人员的能力来组织开发团队
D. 若项目进度滞后于计划，则增加开发人员一定可以加快开发进度

参考答案：(5)A。



要点解析： 在软件项目中开发人员管理是核心的资源，其中人员的配置、调度安排贯穿整个软件项目过程中。人员安排的组织管理是否得当，对软件项目成功起到决定性的作用。在软件项目初始阶段，要根据工作量大小、所需的专业技能类型、团队成员能力水平、性格和开发经验，组建开发小组。整个项目被分解，项目中的成员根据所述的专业组的职能承担项目的相应任务。当项目进度滞后于计划时，下意识的反应往往是增加人力，这是不太可取的，因为在项目中新加入的程序员往往更难融入项目中，所花费的代价会更大。

试题 40 （2015 年下半年试题 6 和试题 7）

某软件项目的活动图如图 12.12 所示，其中顶点表示项目里程碑，连接顶点的边表示活动，边上的数字表示该活动所需的天数，则完成该项目的最少时间为 (6) 天。活动 BD 最多可以晚 (7) 天开始而不会影响整个项目的进度。

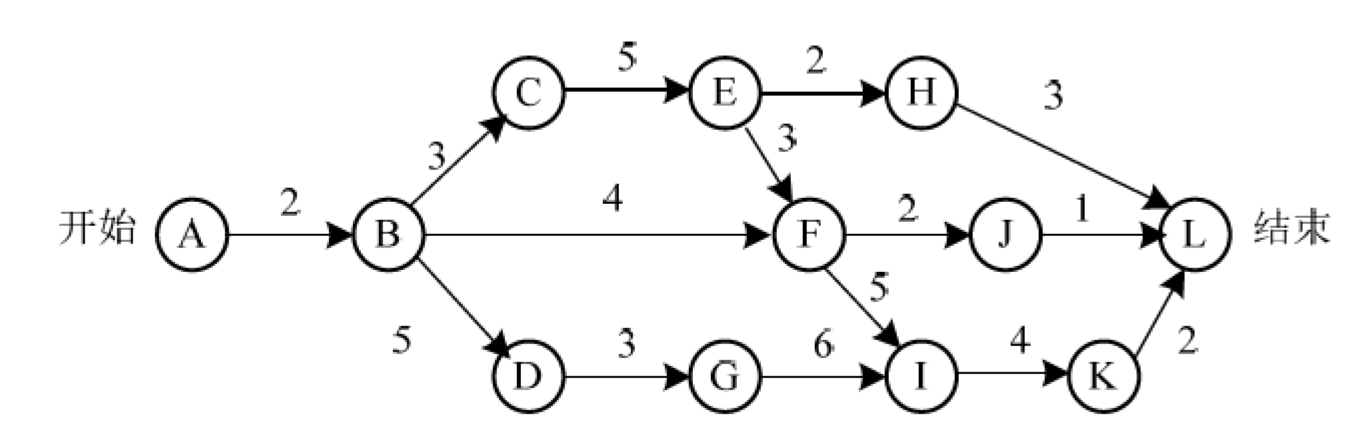


图 12.12　某软件项目的活动图

(6)　A. 9　　B. 15　　C. 22　　D. 24

(7)　A. 2　　B. 3　　C. 5　　D. 9

参考答案： (6)D；(7)A。

要点解析： 本题关键路径为：A→B→C→E→F→I→K→L，是活动图中花费时间最长的活动的序列，长度为 24。BD 在路径 A→B→D→G→I→K→L，长度为 22，比关键路径短 2，因此，要想不影响整个项目的进度，活动 BD 最多可以晚 2 天开始。

试题 41 （2015 年下半年试题 8 和试题 9）

在 Windows 系统中，设 E 盘的根目录下存在 documentl 文件夹，用户在该文件夹下已创建了 document2 文件夹，而当前文件夹为 docunment1。若用户将 test.docx 文件存放在 document2 文件夹中，则该文件的绝对路径为 (8) ；在程序中能正确访问该文件且效率较高的方式为 (9) 。

(8)　A. \document1\　　B. E:\document1\ document2

　　C. document2\　　D. E:\document2\ document1

(9)　A. \document1\test.docx　　B. document1\ document2\test.docx

　　C. document2\test.docx　　D. E:\document1\ document2\test.docx

参考答案： (8)B；(9)C。

要点解析： 绝对路径是指从根目录开始的路径，也称为完全路径；相对路径是指从用户工作目录开始的路径。绝对路径是确定不变的，而相对路径则随着用户工作目录的变化而不断变化。显然，采用相对路径时访问效率较高。

试题 42 （2015 年下半年试题 10）

王某在其公司独立承担了某综合信息管理系统软件的程序设计工作。该系统交付用户、

投入试运行后，王某辞职，并带走了该综合信息管理系统的源程序，拒不交还公司。王某认为，综合信息管理系统源程序是他独立完成的，他是综合信息管理系统源程序的软件著作权人。王某的行为__(10)__。

(10) A. 侵犯了公司的软件著作权　　B. 未侵犯公司的软件著作权
C. 侵犯了公司的商业秘密权　　D. 不涉及侵犯公司的软件著作权

参考答案：(10)A。

要点解析：王某完成的软件是在职期间开发的，因此该软件的著作权归单位享有。他的行为侵犯了公司的著作权。

试题 43 (2015 年上半年试题 1)

某机器字长为 *n* 位的二进制数可以用补码来表示__(1)__有符号定点小数。

(1) A. 2^n　　B. 2^n-1　　C. 2^{n-1}　　D. $2^{n-1}+1$

参考答案：(1)A。

要点解析：机器字长为 *n* 时，补码可表示的定点小数范围为-1～$+(1-2^{-(n-1)})$，一共有 2^n 个数。

试题 44 (2015 年上半年试题 2)

计算机中 CPU 对其访问速度最快的是__(2)__。

(2) A. 内存　　B. Cache　　C. 通用寄存器　　D. 硬盘

参考答案：(2)C。

要点解析：题目中 4 种存储设备按访问速度排序为：通用寄存器> Cache>内存>硬盘。

试题 45 (2015 年上半年试题 3)

计算机中 CPU 的中断响应时间指的是__(3)__的时间。

(3) A. 从发出中断请求到中断处理结束
B. 从中断处理开始到中断处理结束
C. CPU 分析判断中断请求
D. 从发出中断请求到开始进入中断处理程序

参考答案：(3)D。

要点解析：中断响应时间是指计算机接收到中断信号到操作系统做出响应，并完成切换转入中断服务程序的时间。广义上的中断响应时间是指，从来自 CPU 内部或外部的中断信号发生的时刻，到 CPU 完成当前现场保存，而进入此中断信号对应的处理程序的入口处的时刻，所经历的时间。

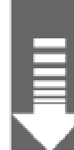
试题 46 (2015 年上半年试题 4)

总线宽度为 32bit，时钟频率为 200MHz，若总线上每 5 个时钟周期传送一个 32bit 的字，则该总线的带宽为__(4)__MB/s。

(4) A. 40　　B. 80　　C. 160　　D. 200

参考答案：(4)C。

要点解析：频率为 200MHz，每 5 个时间周期传一个字，则 1 秒内可传送 200M/5=40 M 次，每次 32bit，4 个字节，得出总线带宽为 40M×4=160MB/s。



试题 47　(2015 年上半年试题 5)

以下关于指令流水线性能度量的叙述中，错误的是__(5)__。

(5)　A. 最大吞吐率取决于流水线中最慢一段所需的时间
　　B. 流水线出现断流，加速比会明显下降
　　C. 要使加速比和效率最大化应该对流水线各级采用相同的运行时间
　　D. 流水线采用异步控制会明显提高其性能

参考答案：(5)D。

要点解析：流水线若采用异步控制方式，流水线输出端任务流出的顺序与输入端任务流入的顺序可以不同，允许后进入流水线的任务先完成，会导致执行顺序混乱，影响程序的执行效率。

试题 48　(2015 年上半年试题 6)

对高级语言源程序进行编译或解释的过程可以分为多个阶段，解释方式不包含__(6)__。

(6)　A. 词法分析　　B. 语法分析
　　C. 语义分析　　D. 目标代码生成

参考答案：(6)D。

要点解析：编译和解释是语言处理的两种基本方式。编译过程包括词法分析、语法分析、语义分析、中间代码生成、代码优化和目标代码生成等阶段，以及符号表管理和出错处理模块。解释过程在词法、语法和语义分析方面与编译程序的工作原理基本相同，但是在运行用户程序时，它直接执行源程序或源程序的内部形式。

这两种语言处理程序的根本区别是：在编译方式下，机器上运行的是与源程序等价的目标程序，源程序和编译程序都不再参与目标程序的执行过程；而在解释方式下，解释程序和源程序(或其某种等价表示)要参与到程序的运行过程中，运行程序的控制权在解释程序。解释器翻译源程序时不产生独立的目标程序，而编译器则需将源程序翻译成独立的目标程序。

试题 49　(2015 年上半年试题 7)

C 程序中全局变量的存储空间在__(7)__分配。

(7)　A. 代码区　　B. 静态数据区　　C. 栈区　　D. 堆区

参考答案：(7)B。

要点解析：代码区：存放函数体的二进制代码。

栈区：由编译器自动分配释放，存放函数的参数值、局部变量的值等。

堆区：一般由程序员分配释放， 若程序员不释放，程序结束时可能由操作系统回收。

静态数据区：内存在程序启动的时候才被分配，而且可能直到程序开始执行的时候才被初始化，所分配的内存在程序的整个运行期间都存在，如全局变量、static 变量等。

试题 50　(2015 年上半年试题 8)

某进程有 4 个页面，页号为 0～3，页面变换表及状态位、访问位和修改位的含义如图 12.13 所示。系统给该进程分配了 3 个存储块，当采用第二次机会页面替换算法时，若访问的页面 1 不在内存，这时应该淘汰的页号为__(8)__。

页号	帧号	状态位	访问位	修改位
0	6	1	1	1
1	—	0	0	0
2	3	1	1	1
3	2	1	1	0

状态位含义 {=0 不在内存；=1 在内存}
访问位含义 {=0 未访问过；=1 访问过}
修改位含义 {=0 未修改过；=1 修改过}

图 12.13　页面变换表

(8)　A. 0　　B. 1　　C. 2　　D. 3

参考答案：(8)D。

要点解析：页面 1 不在内存，可以直接排除选项 B。在本题中，内存中的 3 个页面都是刚刚被访问过的，所以不能以访问位作为判断标准，只能看修改位。修改位中，只有 3 号页未被修改，如果淘汰 3 号页，直接淘汰即可，没有额外的工作要做；如果淘汰 0 号或 2 号，则需要把修改的内容进行更新，这样会有额外的开销。

试题 51　(2015 年上半年试题 9)

王某是某公司的软件设计师，每当软件开发完成后均按公司规定编写软件文档，并提交公司存档，那么该软件文档的著作权__(9)__享有。

(9)　A. 应由公司　　B. 应由公司和王某共同
　　C. 应由王某　　D. 除署名权以外，著作权的其他权利由王某

参考答案：(9)A。

要点解析：王某编写的软件文档属于职务作品，职务作品的著作权应由公司享有。

12.4　强化训练

12.4.1　综合知识试题

试题 1　(2014 年下半年试题 1)

属于 CPU 中算术逻辑单元的部件是__(1)__。

(1)　A. 程序计数器　　B. 加法器　　C. 指令寄存器　　D. 指令译码器

试题 2　(2014 年下半年试题 2)

内存按字节编址从 A5000H 到 DCFFFH 的区域其存储容量为__(2)__。

(2)　A. 123KB　　B. 180KB　　C. 223KB　　D. 224KB

试题 3　(2014 年下半年试题 3)

计算机采用分级存储体系的主要目的是解决__(3)__的问题。

(3)　A. 主存容量不足　　B. 存储器读写可靠性
　　C. 外设访问效率　　D. 存储容量、成本和速度之间的矛盾

试题 4　(2014 年下半年试题 4)

Flynn 分类法基于信息流特征将计算机分成 4 类，其中__(4)__只有理论意义而无实例。

(4)　A. SISD　　B. MISD　　C. SIMD　　D. MIMD

试题 5　(2014 年下半年试题 5)

以下关于结构化系统开发方法的叙述中，不正确的是__(5)__。

(5)　A. 总的指导思想是自顶向下，逐层分解
　　B. 基本原则是功能的分解与抽象
　　C. 与面向对象开发方法相比，更合适大规模、特别复杂的项目
　　D. 特别适合于数据处理领域的项目

试题 6　(2014 年下半年试题 6)

模块 A、B 和 C 包含相同的 5 个语句，这些语句之间没有联系，为了避免重复，把这 5 个模块抽取出来组成模块 D。则模块 D 的内聚类型为__(6)__内聚。

(6)　A. 功能　　B. 通信　　C. 逻辑　　D. 巧合

试题 7　(2014 年下半年试题 7 和试题 8)

图 12.14 是一个软件项目的活动图，其中顶点表示项目里程碑，连接顶点的边表示活动，边的权重表示活动的持续时间，则里程碑__(7)__在关键路径上。活动 GH 的松弛时间是__(8)__。

(7)　A. B　　B. E　　C. C　　D. K

(8)　A. 0　　B. 1　　C. 2　　D. 3

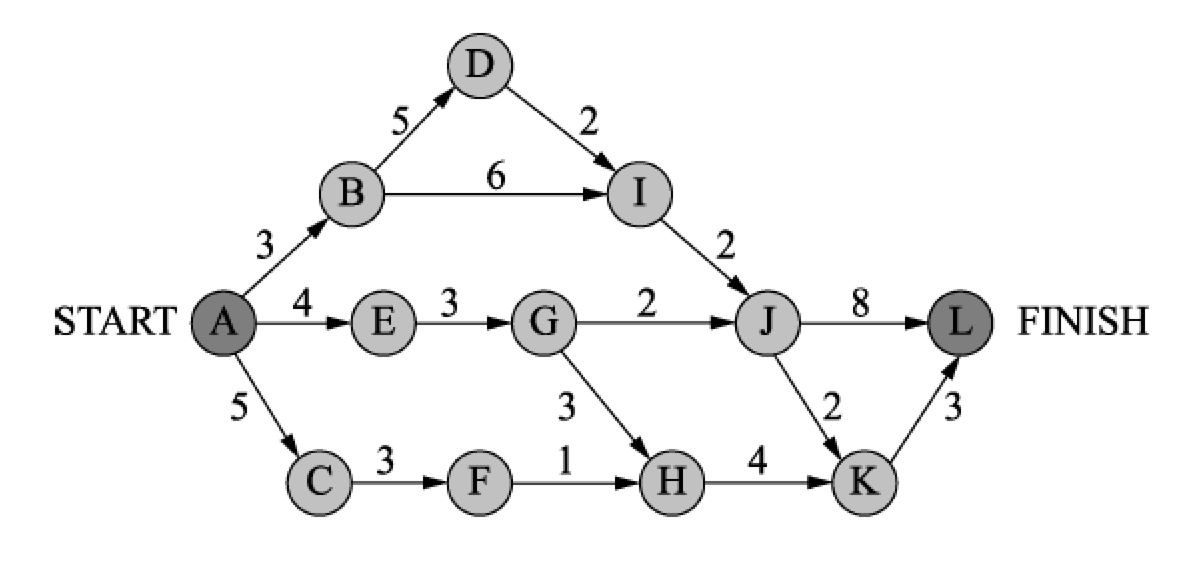


图 12.14　软件项目的活动图

试题 8　(2014 年下半年试题 9)

将高级语言源程序翻译成机器语言程序的过程中，常引入中间代码。以下关于中间代码的叙述中，不正确的是__(9)__。

(9)　A. 中间代码不依赖于具体的机器
　　B. 使用中间代码可提高编译程序的可移植性
　　C. 中间代码可以用树或图表示
　　D. 中间代码可以用栈或队列表示

试题 9　(2014 年下半年试题 10)

甲公司接受乙公司委托开发了一项应用软件，双方没有订立任何书面合同。在此情形下，__(10)__享有该软件的著作权。

(10) A. 甲公司　　B. 甲、乙公司共同　　C. 乙公司　　D. 甲、乙公司均不

试题 10　(2014 年上半年试题 1)

在 CPU 中，常用来为 ALU 执行算术逻辑运算提供数据并暂存运算结果的寄存器是

__(1)__。

(1) A. 程序计数器　B. 状态寄存器　C. 通用寄存器　D. 累加寄存器

试题 11　(2014 年上半年试题 2)

某机器字长为 n，最高位是符号位，其定点整数的最大值为__(2)__。

(2) A. 2^n-1　B. $2^{n-1}-1$　C. 2^n　D. 2^{n-1}

试题 12　(2014 年上半年试题 3 和试题 4)

通常可以将计算机系统中执行一条指令的过程分为取指令、分析和执行指令 3 步。若取指令时间为 $4\Delta t$，分析时间为 $2\Delta t$。执行时间为 $3\Delta t$，按顺序方式从头到尾执行完 600 条指令所需时间为__(3)__Δt；若按照执行第 i 条，分析第 $i+1$ 条，读取第 $i+2$ 条重叠的流水线方式执行指令，则从头到尾执行完 600 条指令所需时间为__(4)__Δt。

(3) A. 2400　B. 3000　C. 3600　D. 5400

(4) A. 2400　B. 2405　C. 3000　D. 3009

试题 13　(2014 年上半年试题 5)

若用 256K×8bit 的存储器芯片，构成地址 40000000H 到 400FFFFFH 且按字节编址的内存区域，则需__(5)__片芯片。

(5) A. 4　B. 8　C. 16　D. 32

试题 14　(2014 年上半年试题 6)

以下关于进度管理工具 Gantt 图的叙述中，不正确的是__(6)__。

(6) A. 能清晰地表达每个任务的开始时间、结束时间和持续时间
B. 能清晰地表达任务之间的并行关系
C. 不能清晰地确定任务之间的依赖关系
D. 能清晰地确定影响进度的关键任务

试题 15　(2014 年上半年试题 7 和试题 8)

若某文件系统的目录结构如图 12.15 所示，假设用户要访问文件 Fault.swf，且当前工作目录为 swshare，则该文件的全文件名为__(7)__，相对路径和绝对路径分别为__(8)__。

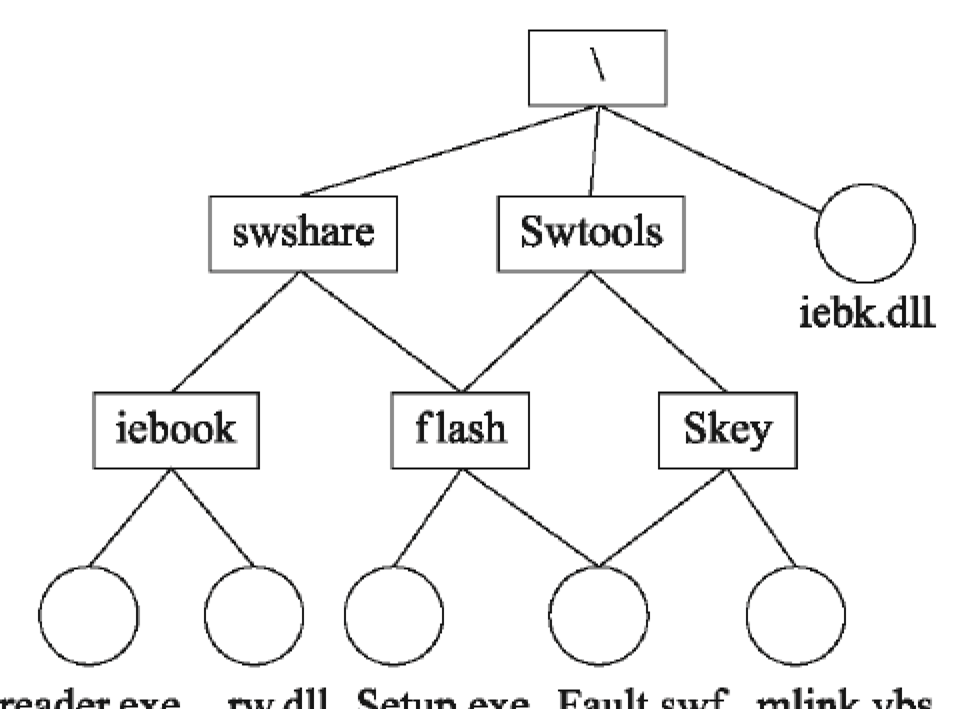


图 12.15　某文件系统的目录结构



(7)　A. Fault.swf　　　　　　　　B. flash\Fault.swf
　　 C. swshare\flash\Fault.swf　　D. \swshare\flash\Fault.swf

(8)　A. swshare\flash\和\flash\　　B. flash\和\swshare\flash\
　　 C. \swshare\flash\和 flash\　　D. \flash\和\swshare\flash\

试题 16　(2014 年上半年试题 9)

在引用调用方式下进行函数调用是将__(9)__。

(9)　A. 实参的值传递给形参　　B. 实参的地址传递给形参
　　 C. 形参的值传递给实参　　D. 形参的地址传递给实参

试题 17　(2014 年上半年试题 10)

王某买了一幅美术作品原件，则他享有该美术作品的__(10)__。

(10) A. 著作权　　B. 所有权　　C. 展览权　　D. 所有权与其展览权

12.4.2　综合知识试题参考答案

【试题 1】答　案：(1)B。

解　析：运算器由算术逻辑单元(ALU)、累加寄存器、数据缓冲寄存器和状态条件寄存器组成。累加寄存器简称累加器。程序计数器、指令寄存器、指令译码器都属于控制器。

【试题 2】答　案：(2)D。

解　析：存储容量为 DCFFFH – A5000H + 1H = 38000H = 0011 1000 0000 0000 0000 B = 224KB。

【试题 3】答　案：(3)D。

解　析：为了解决对存储器要求容量大、速度快、成本低三者之间的矛盾，目前通常采用多级存储器体系结构，即使用高速缓冲存储器、主存储器和外存储器。高速缓冲存储器：高速存取指令和数据，存取速度快，但存储容量小。主存储器：主存存放计算机运行期间的大量程序和数据，存取速度较快，存储容量不大。外存储器：外存存放系统程序和大型数据文件及数据库，存储容量大、成本低。

【试题 4】答　案：(4)B。

解　析：按照 Flynn 分类法，根据计算机中指令和数据的并行状况可把计算机分成以下几种。

单指令流单数据流(SISD)——传统的计算机包含单个 CPU，它从存储在内存中的程序那里获得指令，并作用于单一的数据流。

单指令流多数据流(SIMD)——单个的指令流作用于多于一个的数据流上。例如有数据 4、5 和 3、2，一个单指令执行两个独立的加法运算：4+5 和 3+2，就被称为单指令流多数据流。SIMD 的一个例子就是一个数组或向量处理系统，它可以对不同的数据并行执行相同的操作。

多指令流单数据流(MISD)——用多个指令作用于单个数据流的情况，实际上很少见。这种冗余多用于容错系统。

多指令流多数据流(MIMD)——这种系统类似于多个 SISD 系统。实际上，MIMD 系统

的一个常见例子是多处理器计算机，如 Sun 公司的企业级服务器。

【试题 5】答　案：(5)C。

解　析：结构化系统开发方法(Structured System Development Methodology)是目前应用得最普遍的一种开发方法，是一种面向数据流的开发方法。其基本思想是用系统的思想和系统工程的方法，按照用户至上的原则结构化、模块化，自顶向下对系统进行分析与设计。结构化方法特别适合于数据处理领域的问题，但是不适用于规模较大、比较复杂的系统开发。

【试题 6】答　案：(6)D。

解析：内聚按紧密程度从低到高排列次序为偶然内聚、逻辑内聚、时间内聚、过程内聚、通信内聚、信息内聚、功能内聚。

偶然内聚：又称巧合内聚，完成一组没有关系或松散关系的任务。

逻辑内聚：完成逻辑上相关的一组任务。

时间内聚：所包含的任务必须在同一时间间隔内执行(如初始化模块)。

过程内聚：处理元素相关，而且必须按待定的次序执行。

通信内聚：所有处理元素集中在一个数据结构的区域上。

信息内聚：处理元素相同，而且必须顺序执行。

功能内聚：完成一个单一功能，各个部分协同工作，缺一不可。

题目中，5 个模块之间没有联系，可见是巧合内聚。

【试题 7】答　案：(7)A；(8)D。

解　析：关键路径通常是决定项目工期的进度活动序列。它是项目中最长的路径，即使很小浮动也可能直接影响整个项目的最早完成时间。本题最长的路径为 A-B-D-I-J-L，持续时间为 20。

松弛时间为最早开始时间(ES)与最迟开始时间(LS)之差，或者最早结束时间(EF)与最迟结束时间(LF)之差。先从前往后，算每个活动最早开始时间、最早结束时间。再从后往前算每个活动最晚结束时间和最晚开始时间。GH 活动最早开始时间是 7，最晚开始时间是 10，所以松弛时间是 3。

【试题 8】答　案：(9)D。

解　析：中间代码表达了程序执行流程和状态转换图，通常用树或图表示。

【试题 9】答　案：(10)A。

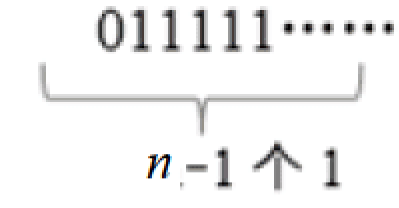
解　析：接受任务开发软件的著作权归属一般按以下两条标准确定：①在合同中明确约定的，按照合同约定实行；②未明确约定的，著作权属于实际完成软件开发的单位。

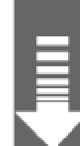
【试题 10】答　案：(1)D。

解　析：在运算器中，累加寄存器是专门存放算术或逻辑运算的一个操作数和运算结果的寄存器，能进行加、减、读出、移位、循环移位和求补等操作，是运算器的主要部分。

【试题 11】答　案：(2)B。

解　析：由于最高位是符号位，因此最大的定点整数是：





最高位 0 表示正数，值为 $2^0+2^1+2^2+\cdots+2^{n-2}=2^{n-1}-1$。

【试题 12】答　案：(3)D；(4)B。

解　析：按顺序方式需要执行完一条执行之后再执行下一条指令，执行 1 条执行所需的时间为 $4\Delta t+2\Delta t+3\Delta t=9\Delta t$，执行 600 条指令所需的时间为 $9\Delta t\times600=5400\Delta t$。

若采用流水线方式，则处理过程如图 12.16 所示。可见执行完 600 条执行所需要的时间为 $4\Delta t\times600+2\Delta t+3\Delta t=2405\Delta t$。

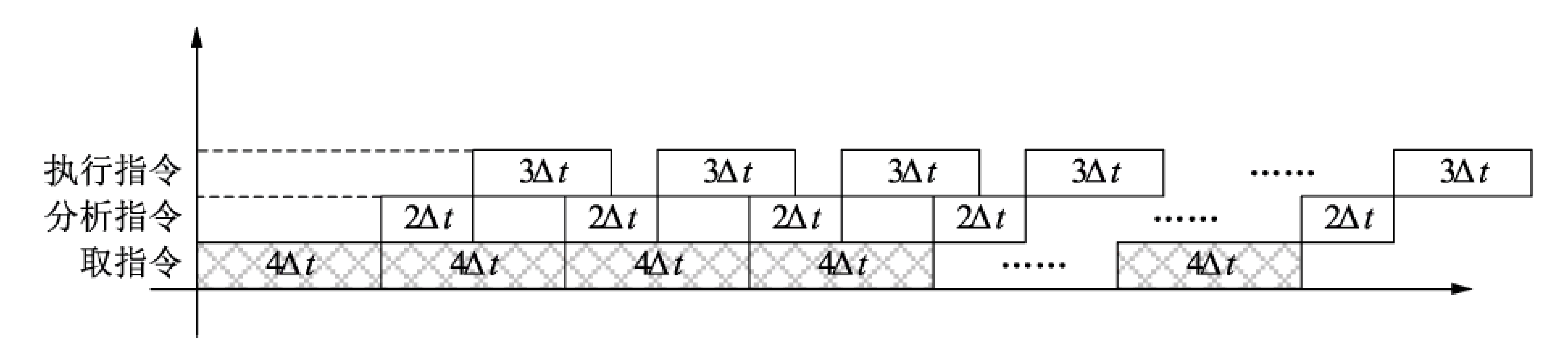


图 12.16　采用流水线方式的处理过程

【试题 13】答　案：(5)A。

解　析：内存区域从 40000000H 到 400FFFFFH，占用的字节数为

400FFFFFH−40000000H+1=100000H=1 0000 0000 0000 0000 0000B=2^{20}=1024K

一片 256K×8bit 的存储器芯片的存储容量为 256KB，需要的芯片数为 1024÷256=4。

【试题 14】答　案：(6)D。

解　析：甘特图内在思想简单，即以图示的方式通过活动列表和时间刻度形象地表示出任何特定项目的活动顺序与持续时间。基本图形是一条线条图，横轴表示时间，纵轴表示活动(项目)，线条表示在整个期间上计划和实际的活动完成情况。它直观地表明任务计划在什么时候进行，以及实际进展与计划要求的对比。管理者由此可便利地弄清一项任务(项目)还剩下哪些工作要做，并可评估工作进度。

优点：能清晰地描述每个任务从何时开始，到何时结束以及各个任务之间的并行性。

缺点：不能清晰地反映出个任务之间的依赖关系，难以确定整个项目的关键所在，也不能反映计划中有潜力的部分。

【试题 15】答　案：(7)D；(8)B。

解　析：全文件名应该从根目录开始，因此为\swshare\flash\fault.swf。相对路径是从当前路径开始的路径，fault.swf 在当前工作目录 swshare 下的 flash 文件夹中，因此相对路径为 flash\。绝对路径是指从根目录开始的路径，即\swshare\flash\。

【试题 16】答　案：(9)B。

解析：引用调用是把实参(如 int a)的地址(&a)赋给形参(指针变量，比如*b，这时 b=&a，即 b 指向变量 a)，如果*b(也即 a 对应的内存空间)发生变化，也就是变量 a 的值发生了变化。

【试题 17】答　案：(10)D。

解　析：很显然，作品的买卖导致了所有权的转移，著作权法第十八条规定：“美术等作品原件所有权的转移，不视为作品著作权的转移，但美术作品原件的展览权由原件所有人享有。”因此，作品交易后，著作权仍归原作者，王某享有购买的美术作品的所有权和其展览权。

第 13 章 计算机专业英语

13.1 备考指南

13.1.1 考纲要求

根据考试大纲中相应的考核要求，在“计算机专业英语”知识模块上，要求考生掌握以下方面的内容。

(1) 具有工程师所要求的英语阅读水平。

(2) 掌握本领域的基本英语词汇。

13.1.2 考点统计

“计算机专业英语”知识模块在历次网络工程师考试试卷中出现的考核知识点及分值分布情况如表 13.1 所示。

表 13.1　历年考点统计表

年　份	题　号	知 识 点	分　值
2017 年下半年	上午：71～75	计算机网络专业英语	10 分
	下午：无		0 分
2017 年上半年	上午：71～75	计算机网络专业英语	10 分
	下午：无		0 分
2016 年下半年	上午：71～75	计算机网络专业英语	10 分
	下午：无		0 分

续表

年　份	题　号	知 识 点	分　值
2016 年上半年	上午：71～75	计算机网络专业英语	10 分
	下午：无		0 分
2015 年下半年	上午：71～75	计算机网络专业英语	10 分
	下午：无		0 分
2015 年上半年	上午：71～75	计算机网络专业英语	10 分
	下午：无		0 分
2014 年下半年	上午：71～75	计算机网络专业英语	10 分
	下午：无		0 分
2014 年上半年	上午：71～75	计算机网络专业英语	10 分
	下午：无		0 分
2013 年下半年	上午：71～75	计算机网络专业英语	10 分
	下午：无		0 分
2013 年上半年	上午：71～75	计算机网络专业英语	10 分
	下午：无		0 分
2012 年下半年	上午：71～75	计算机网络专业英语	10 分
	下午：无		0 分
2012 年上半年	上午：71～75	计算机网络专业英语	10 分
	下午：无		0 分

13.1.3　命题特点

纵观历年试卷，本章知识点是以选择题的形式出现在试卷中的。本章知识点在历次考试上午试卷中，所考查的题量为 5 道选择题，所占分值为 5 分(约占试卷总分值 75 分中的 6.7%)。本章考题主要检验考生的阅读水平以及考生是否掌握了计算机网络领域的词汇，考试难度较低。

13.2　考点串讲

英语词汇是最基础的部分，由于计算机网络是不断更新的领域，新的思想不断涌现，因而也伴随着新的词汇出现。由于新出现的词汇和网络技术的专业性，往往造成理解上的偏差，因此需要应试者在基本了解网络技术中英语专业词汇的基础上，将英语词汇和汉语词汇在功能和语义上相对应，形成正确的理解。

应试者需要准确掌握词语的意义，区分同义词在意义和使用上的差别；准确掌握名词单、复数形式，以及由单、复数形式带来不同语义的解释；准确掌握关系代词、关系副词、联系词在语句乃至整个语篇中的逻辑意义。

在词汇复习中，尤其需要注意专业词汇的缩写，这些缩写往往是某些技术、设备或协议的代称，在整个试题中是核心词汇。复习时应多读一些计算机网络方面的英语时文。解

题时，一般先考虑语义，后考虑语法。

13.2.1 计算机网络技术基本词汇

下面列出常用的计算机网络技术基本术语，供考生复习时参考。

accept 接受
access control 访问控制
acknowledgement(ACK) 确认
adaptive routing 自适应路由
address field 地址字段
amplitude 振幅
analog signal 模拟信号
anonymous FTP 匿名 FTP
application layer 应用层
asynchronous 异步
backbone 主干
bandwidth 带宽
baseband mode 基带模式
baud rate 波特率
binary exponential backoff algorithm 二进制指数退避算法
bit-oriented protocol 面向比特的协议
block check character 块校验字符
Border Gateway Protocol 边界网关协议
bridge 网桥
client 客户
client/server model 客户/服务器模式
coaxial cable 同轴电缆
code 编码
common bus topology 公共总线拓扑结构
common gateway 公共网关接口
Common Management Information Protocol 通用管理信息协议
communications subnet 通信子网
compact disc 光盘
compression 压缩
congestion 拥塞
connection 连接
contention 竞争
contention protocol 竞争协议
control bits 控制位
control character 控制字符
Data Circuit-Terminating Equipment(DCE) 数据电路端接设备
Data Encryption Standard(DES) 数据加密标准
bridge protocol data unit 网桥协议数据单元
broadcast address 广播地址
brouter 桥路器
buffering 缓冲
cable modem 电缆调制解调器
Caesar cipher 凯撒密码
call confirmation 呼叫证实
call request 呼叫请求
Carrier Sense Multiple Access(CSMA) 载波侦听多路访问
Carrier Sense Multiple Access with Collision Detection (CSMA/CD) 带冲突检测的载波侦听多路访问
carrier signal 载波信号
cell 信元
channel 信道
checksum 校验和
choke packet 抑制分组
ciphertext 密文
circuit switching 电路交换
file server 文件服务器
File Transfer Protocol 文件传输协议
filter 滤波器
flow control 流量控制
fragment 段
fragmentation 分段
frame 帧
frequency 频率
frequency-division multiplexing 频分多路复用
full duplex 全双工
gateway 网关
graded-index multimode fiber 级率多模光纤
hacker 黑客
half duplex 半双工
Hamming code 海明码
handshaking 握手
High-level Data Link Control(HDLC) 高级数据链路控制协议
host 主机
Hypertext Transfer Protocol(HTTP) 超文本传输协议
infrared light 红外线

data link layer 数据链路层
datagram 数据报
decryption 解密
demodulation 解调
destination address 目的地址
differential encoding 差分编码
digital signal 数字信号
digital signature 数字签名
directory service 目录服务
domain 域
Domain Name System 域名系统
echo reply 回送响应
echo request 回送请求
electronic mail(E-mail) 电子邮件
encryption 加密
encryption key 密钥
error control 差错控制
error correction 差错校正
error detection 差错检测
Ethernet 以太网
even parity 偶校验
exterior gateway protocol 外部网关协议
fiber distributed data interface 光纤分布式数据接口
network virtual terminal 网络虚拟终端
non-persistent CSMA 非坚持 CSMA
Nyquist theorem 尼奎斯特定理
octet 字节
odd parity 奇校验
Open Systems Interconnect(OSI) 开放系统互连
packet 分组
packet header 分组头
packet-switched network 分组交换网络
parity bit 奇偶校验位
path 通路
path control 通路控制
physical layer 物理层
pixels 像素
plaintext 明文
prefix 前缀
presentation layer 表示层
protocol 协议
pulse amplitude modulation 脉冲幅度调制
pulse code modulation 脉码调制
radio 无线电收发机
receiving window 接收窗口
Internet 因特网
Internet Control Message Protocol (ICMP) 网际控制报文协议
Internet Protocol 网际协议
Internet worm 因特网蠕虫
key exchange 密钥交换
laser 激光
Local Area Network(LAN) 局域网
local exchange 本地交换局
local loop 本地回路
Manchester code 曼彻斯特编码
Medium Access Control(MAC) 媒体访问控制
message handling 报文处理
message transfer protocol 报文传送协议
modem 调制解调器
modulation 调制
multiplexer 多路复用器
network 网络
Network Control Protocol 网络控制协议
Network Interface Card(NIC) 网络接口卡
network layer protocol 网络层协议
network topology 网络拓扑结构
Simple Mail Transfer Protocol(SMTP) 简单邮件传输协议
simplex 单工
single-mode fiber 单模光纤
sliding window 滑动窗口协议
socket 套接字
source address 源地址
source quench 源抑制
spanning tree algorithm 生成树算法
start bit 起始位
start of frame delimiter 帧起始定界符
static routing 静态路由
stop bit 停止位
subnet 子网
successor 后继
switch 交换机
SYN character 同步字符
synchronous 同步
Synchronous Optical Network(SONET) 同步光纤网
telegraph 电报
terminal adapter 终端适配器
three-way handshake 三次握手
time exceeded 超时

remote logins 远程登录
repeater 中继器
reply 应答
root bridge 根网桥
root port 根端口
route 路由
router 路由器
routing algorithm 路由算法
Routing Information Protocol 路由信息协议
routing table 路由表
sampling frequency 采样率
satellite 人造卫星
script 脚本
security 安全
segment 段
sequence number 序列号
serial transmission 串行传输
server 服务器
session 会话
session control 会话控制
session layer 会话层
signal-to-noise ratio 信噪比
time to live 生存期
time-division 时分
multiplexing 多路复用
timestamp reply 时戳应答
timestamp request 时戳请求
token 令牌
transceiver 收发器
transmission rate 传输速率
transparent bridge 透明网桥
transport layer 运输层
twisted pair 双绞线
tunneling 隧道
Uniform Resource Locator(URL) 统一资源定位器
User Datagram Protocol(UDP)用户数据报协议
verification 验证
virtual circuit(route) 虚电路(路由)
virus 病毒
Wide Area Network(WAN) 广域网
window 窗口
World Wide Web 万维网
worm 蠕虫

13.2.2 专业英语试题分析

上午科目的第71～75题一般是完形填空的形式，主要考查应试者结合计算机专业技术知识对全文综合理解的程度和串联上下文的能力；应试者语法知识和对句法结构的辨识能力；应试者的词汇量和词汇运用能力。

具体而言，完形填空主要考查应试者对语篇中句法、词语和短语的把握能力，具有较强的测试性。每一个空处都要通过上下文进行综合考虑，仅仅依靠一个单句往往无法确定正确选项。

语篇的内容往往是对网络技术中协议、通信过程、设备、最新技术等相关知识的描述，需要应试者对这些内容有一定的了解。

13.2.2.1 完形填空中的句法

计算机英语的完形填空，句法强调时态、语态、倒装、复合，同时要求主语、谓语和宾语结构在数、格等方面一致。此外，连接手段包括关系代词、关系副词、连接词等，要求与整个语篇的行文相一致，起到或承接，或转折，或加强的作用，有着非常突出的个性特征。

时态在描述某项事务的发展历史时，一般采用过去时态；对目前尚在使用中的技术，采取完成时态或现在时；而对未来技术的展望，大都采用将来时。句中几个受同一时间状态限制的动词时态在表达形式上要保持一致，这里包括并列的谓语动词以及主句和从句中

谓语动词在表达形式上的一致。

计算机英语的语篇在描述技术类知识时，语态一般力求客观，采用描述性和被动语态较多。这里要注意只有及物动词及相当于及物动词的词组才有被动语态的表达形式。在并列结构中，同样的语义往往需要同样的语态表达形式。

13.2.2.2　完形填空中的短语和固定用法

英语中有相当数量的动词短语、介词短语和固定搭配，其来源广泛，搭配方式丰富多变。因此需要应试者从动词入手，熟悉固定搭配，尤其是动词短语；从介词入手，了解介词本身的意义，进而了解同一个介词与不同动词、名词搭配产生的不同或相关的意义；理解固定搭配的外延，增强对语义提示的审查力。

13.2.2.3　完形填空的答题要领

(1) 通过首句或出现的核心词汇来推断全文的信息。短文的首句往往是主题句，或出现了核心词汇，能为理解文章的大意和主要内容提供必要线索。一般首句还提供背景资料，因此要特别注意首句，抓住整个段落的纲要。

(2) 把握文章发展的基本线索。文章总是按照一定思路发展起来的，而不同的逻辑关系主要依靠使用逻辑连接词来表达的。文章如果没有出现内在的逻辑关系，就会出现语义不清、逻辑混乱。所以通过表示逻辑关系的词汇把握文章发展的基本线索是至关重要的。

(3) 借助语法知识和专业背景知识确定正确的词汇选项。计算机专业英语词汇的考查在试题中占一定比例，词汇选项的设计和文章难度的制定与语法都息息相关。应试者务必借助语法知识和专业背景知识来确定正确的词汇选项，同时注意填入的词汇和文中句子的结构要求相一致。

13.2.2.4　完形填空的答题步骤

(1) 通读全文。由于完形填空是在考查全面理解内容的基础上运用语言的能力，试题篇幅又较短，所以应试者完全有时间利用通读对全文内容有一个基本的了解。应试者要快速阅读段落，把握基本观点，通读时以浏览为主，可以忽略细节。

(2) 复读答题。在通读的基础上，应试者最好能立即复读，并结合选项，从语法结构、语义、词义、固定搭配等方面结合专业知识来考虑选项。选定之后，还需要回读。在整个答题过程中，切记全文的整体意义，保持思路的连贯性，从而做出最合适的正确选择。

(3) 重读检查。在确定了所有选项以后，一定要重读全文，检查并核实每个选项在整篇文章中没有造成语义、结构、逻辑等方面的差错，确保短文是一个内容连贯、层次清晰、中心思想突出的整体。

13.3　真题详解

试题 1　(2017 年下半年试题 71 ~ 试题 75)

Routing in circuit-switching networks has traditionally involved a static routing strategy with

the use of (71) paths to respond to increased load. Modern routing strategies provide more adaptive and flexible approaches. The routing function of a packet-switching network attempts to find the least-cost route through the network , with cost based on the number of (72) expected delay, or other metrics in virtually all packet-switching networks, some sort f adaptive routing technique is used. Adaptive routing algorithms typically rely on the (73) information about traffic conditions among nodes. In most cases, adaptive strategies depend n status information that is (74) at one place but used at another. There is a tradeoff here tween the quality of the information and the amount of (75) . The exchanged information itself a load on the constituent networks , causing a performance degradation.

(71) A. only　B. single　C. alternate　D. series
(72) A. hops　B. sites　C. members　D. points
(73) A. exchange　B. transportation　C. reception　D . transmission
(74) A. rejected　B. collected　C. discarded　D. transmitted
(75) A. packets　B. information　C. data　D. overhead

参考答案：(71)B；(72)A；(73)A；(74)B；(75)A。

参考译文：电路交换网络中的路由传统上涉及静态路由策略，使用单一路径来响应增加的负载。现代路由策略提供了更灵活和更灵活的方法。分组交换网络的路由功能试图通过网络发现成本最低的路由，其成本基于跳数、预期的延迟或其他度量。在几乎所有的分组交换网络中，使用某种自适应路由技术。自适应路由算法通常依赖于有关节点之间流量情况的信息。在大多数情况下，适应策略依赖于在一个地方收集但在另一个地方使用的状态信息。在信息质量和数据包数量之间有一个折中。交换的信息本身成为构成网络上的负载，导致性能下降。

试题 2 (2017 年上半年试题 71～试题 75)

If two communicating entities are indifferent hosts connected by a network，there is a risk that PDUs will not arrive in the order in which they were sent，because they may traverse (71) paths through the network. If each PDUs is given a unique number，and numbers are assigned (72) , then it is a logically simple task for the receiving entity to reorder (73) PDUs on the basis of sequence number. A problem with this scheme is that，with a (74) sequence number field，sequence number will repeat. Evidently, the maximum sequence number must be (75) than the maximum number of PDUs that could be outstanding at anytime.

(71) A. same　B. different　C. single　D. unique
(72) A. randomly　B. equally　C. uniformly　D. sequentially
(73) A. received　B. sent　C. transmitting　D. forwarding
(74) A. various　B. diverse　C. finite　D. infinite
(75) A. smaller　B. greater　C. less　D. more

参考答案：(71)B；(72)D；(73)A；(74)C；(75)B。

参考译文：如果两个通信实体是通过网络连接的无关主机，则存在这样的风险，即 PDU 不会按照它们发送的顺序到达，因为它们可能通过网络穿过不同的路径。如果给每个 PDU 赋予唯一的号码，则数字被顺序地分配，那么接收实体根据序号对接收到的 PDU 进行重新

排序是一个逻辑上简单的任务。该方案的问题在于，在有限的序列号字段中，序列号将重复。显然，最大序列号必须大于 PDU 的最大数量才能在任何时候都展示出卓越。

试题 3 （2016 年下半年试题 71～试题 75）

All three types of cryptography schemes have unique function mapping to specific applications. For example, the symmetric key (71) approach is typically used for the encryption of data providing (72) , whereas asymmetric key cryptography is mainly used in key (73) and nonrepudiation , thereby providing confidentiality and authentication. The hash (74) (noncryptic), on the other hand, does not provide confidentiality but provides message integrity, and cryptographic hash algorithms provide message (75) and identity of peers during transport over insecure channels.

(71) A.cryptography　　B. decode　　C. privacy　　D. security
(72) A.conduction　　B. confidence　　C. confidentiality　　D. connection
(73) A.authentication　　B. structure　　C. encryption　　D. exchange
(74) A.algorithm　　B. secure　　C. structure　　D. encryption
(75) A.confidentially　　B. integrity　　C. service　　D. robustness

参考答案：(71)A；(72)C；(73)C；(74)A；(75)A。

参考译文：所有三种类型的密码方案都具有映射到特定应用的独特功能。例如，对称密钥加密方法通常用于保障加密数据的保密性，而非对称密钥加密主要用于密钥加密和不可否认性，从而提供机密性和身份认证。另外，散列算法(非加密)不提供机密性，但提供了消息完整性，而带密钥的哈希算法保障数据的完整性并且能够为点对点信息通过不安全信道传递时提供身份验证。

试题 4 （2016 年上半年试题 71～试题 75）

Without proper safeguards, every part of a network is vulnerable to a security breach or unauthorized activity from (71) , competitors, or even employees. Many of the organizations that manage their own (72) network security and use the Internet for more than just sending/receiving E-mails experience a network (73) —and more than half of these companies do not even know they were attacked. Smaller (74) are often complacent, having gained a false sense of security. They usually react to the last virus or the most recent defacing of their website. But they are trapped in a situation where they do not have the necessary time and (75) to spend on security.

(71) A. intruders　　B. terminals　　C. hosts　　D. users
(72) A. exterior　　B. internal　　C. centre　　D. middle
(73) A. attack　　B. collapse　　C. breakdown　　D. virus
(74) A. users　　B. campuses　　C. companies　　D. networks
(75) A. safeguards　　B. businesses　　C. experiences　　D. resources

参考答案：(71)A；(72)B；(73)A；(74)C；(75)D。

参考译文：如果没有适当的保护措施，网络的每个部分都容易受到来自入侵者、竞争对手，甚至是员工的安全漏洞或未经授权的攻击。很多组织管理自己的内部网络安全并使用

Internet 不仅仅是发送/接收电子邮件遭遇网络攻击，其中一半以上的公司甚至不知道遭到攻击。小公司常常自满，已经获得了虚假的安全感。他们通常会对最后一个病毒或最近的恶意网站做出反应，但他们被困在一个情况下，即他们没有必要的时间和资源专注于安全防护。

试题 5 (2015 年下半年试题 71～试题 75)

The Dynamic Host Configuration Protocol provides configuration parameters to Internet (71) . DHCP consists of two components: a (72) for delivering host-specific configuration parameters from a DHCP server to a host and a mechanism for allocation of network addresses to hosts. DHCP is built on a client-server model, where designated DHCP server hosts allocate network addresses and deliver (73) parameters to dynamically configured hosts. DHCP supports three mechanisms for IP address allocation. In “automatic allocation”, DHCP assigns a (74) IP address to a client. In “dynamic allocation”, DHCP assigns an IP address to a client for a limited period of time. In “manual allocation”, a client’s IP address is assigned by the network (75) , and DHCP is used simply to convey the assigned address to the client.

(71) A. switch　B. terminal　C. hosts　D. users
(72) A. router　B. protocol　C. host　D. mechanism
(73) A. control　B. broadcast　C. configuration　D. transmission
(74) A. permanent　B. dynamic　C. connection　D. session
(75) A. controller　B. user　C. host　D. administrator

参考答案：(71)C；(72)B；(73)C；(74)A；(75)D。

参考译文：动态主机配置协议为互联网上的主机提供配置参数。DHCP 由两部分组成：传递从 DHCP 服务器至主机的具体配置参数的协议以及主机网络地址分配机制。DHCP 是建立在客户机-服务器模型之上的，由指定的 DHCP 服务器向动态配置的主机分配网络地址和传递配置参数。DHCP 支持三种 IP 地址分配机制。在“自动分配”机制中，DHCP 分配给客户端一个永久地址。在“动态分配”机制中，DHCP 分配给客户端一个临时性的 IP 地址。在“手动配置”机制中，客户端的 IP 地址是由网络管理员分配，DHCP 仅仅起到配送这个指定的地址给客户端的作用。

试题 6 (2015 年上半年试题 71～试题 75)

Traditional network layer packet forwarding relies on the information provided by network layer (71) protocols, or static routing, to make an independent forwarding decision at each (72) within the network. The forwarding decision is based solely on the destination (73) IP address. All packets for the same destination follow the same path across the network, if no other equal-cost (74) exist. Whenever a router has two equal-cost paths toward a destination, the packets toward the destination might take one or both of them, resulting in some degree of load sharing. Enhanced Interior Gateway Routing Protocol (EIGRP) also supports non-equal-cost (75) sharing although the default behavior of this protocol is equal-cost. You must configure EIGRP variance for non-equal-cost load balancing.

(71) A. switching　B. signaling　C. routing　D. session
(72) A. switch　B. hop　C. host　D. customer

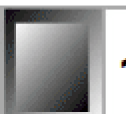


(73) A. connection　B. transmission　C. broadcast　D. customer
(74) A. paths　B. distance　C. broadcast　D. session
(75) A. loan　B. load　C. content　D. constant

参考答案：(71)C；(72)B；(73)D；(74)A；(75)B。

参考译文：传统的网络层数据包的转发依赖于网络层路由协议提供的信息，或者静态路由，独立决定网络内每一跳的转发决策。转发决策仅仅基于目的客户机的 IP 地址。如果不存在等价的路径，则相同目的地的数据包将沿相同的路径在网络中转发。每当路由器有两条等价的路径通往目的地，数据包可能会选择其中的一条或者两条到达目的地，在一定程度上均衡了负载。增强内部网关路由协议(EIGRP)也支持非等价的负载分担，尽管这个协议默认是等价的。你必须配置 EIGRP 非等价负载均衡的方差。

13.4　强化训练



13.4.1　综合知识试题

试题 1　(2014 年下半年试题 71～试题 75)

CDMA for cellular systems can be described as follows. As with FDMA, each cell is allocated a frequency__(71)__, which is split into two parts: half for reverse (mobile unit to base station) and half for__(72)__(base station to mobile unit). For full-duplex__(73)__, a mobile unit uses both reverse and forward channels. Transmission is in the form of direct-sequence spread __(74)__which uses a chipping code to increase the data rate of the transmission, resulting in an increased signal bandwidth. Multiple access is provided by assigning__(75)__chipping codes to multiple users, so that the receiver can recover the transmission of an individual unit from multiple transmissions.

(71) A. wave　B. signal　C. bandwidth　D. domain
(72) A. forward　B. reverse　C. backward　D. ahead
(73) A. connection　B. transmission　C. compromise　D. communication
(74) A. structure　B. spectrum　C. stream　D. strategy
(75) A. concurrent　B. orthogonal　C. higher　D. lower

试题 2　(2014 年上半年试题 71～试题 75)

The traditional way of allocating a single channel, such as a telephone trunk, among multiple competing users is to chop up its__(71)__by using one of the multiplexing schemes, such as FDM. If there are N users, the bandwidth is divided into N equal-sized portions, with each user being assigned one portion. Since each user has private frequency__(72)__, there is now no interference among users. When there is only a small and constant number of users, each of which has a steady stream or heavy load of__(73)__this division is a simple and efficient allocation mechanism. A wireless example is FM radio stations. Each station gets a portion of the FM band and uses it most

of the time to broadcast its signal. However when the number of senders is large and varying or the traffic is (74), FDM presents some problems. If the spectrum is cut up into N regions and fewer than N users are currently interested in communicating, a large piece of valuable spectrum will be wasted. And if more than N users want to communicate, some of them will be denied (75) for lack of bandwidth, even if some of the users who have been assigned a frequency band ever transmit or receive anything.

(71) A. capability	B. capacity	C. ability	D. power
(72) A. band	B. range	C. domain	D. assignment
(73) A. traffic	B. data	C. information	D. communications
(74) A. continuous	B. steady	C. busy	D. flow
(75) A. allowance	B. connection	C. percussion	D. permission

13.4.2 综合知识试题参考答案

【试题1】答　案：(71)C；(72)A；(73)D；(74)B；(75)B。

参考译文：蜂窝系统中的CDMA可以描述如下：采用FDMA，每个蜂窝分配有一频率带宽，该频率带宽被分成两部分，一部分用于反向传输(移动单元到基站)，一部分用于正向传输(基站到移动单元)。为了实现双工通信，一个移动单元要使用正向和反向两个信道。传输是以直接序列扩频的形式进行的，并使用码片序列来增加数据传输的速率，进而导致信号带宽增加。采用多路存取技术将正交的码片序列分配给多个用户，因此接收者可以从多路传输中恢复自己的传输单元。

【试题2】答　案：(71)B；(72)B；(73)A；(74)C；(75)D。

参考译文：传统的分配信号的方法，比如电话中继，多个竞争用户使用一种多路复用方案分配信道的容量，如FDM。如果有 *N* 个用户，带宽将被分成 *N* 个同样大小的部分，每个用户将分得一部分。既然每个用户都有自己的频率范围，因此用户之间没有干扰。当用户数量少且不变，每个用户将保持稳定的数据流和通信负载，这种划分是一种简单而高效的分配机制。FM广播电台是一个无线的例子。每个电台分配有一个FM频带，大部分时间用它来广播信号。但是，当发送者的数量很多且是变化的，或者通信很忙，FDM将会有一些问题。如果频谱被分成 *N* 个区域，而不足 *N* 个用户在通信，大量宝贵的频谱会被浪费。如果超过 *N* 个用户想要通信，他们中一些人的通信将会因为带宽的不足而被拒绝，即使一些用户已经分配了某一频率的带宽参与过发送或接收数据。

第 14 章 考前模拟卷、答案与解析

14.1 考前模拟卷

14.1.1 考前模拟卷 1

上午科目

● 若内存地址区间为 4000H～43FFH，每个存储单元可存储 16 位二进制数，该内存区域由 4 片存储器芯片构成，则构成该内存所用的存储器芯片的容量是 (1) 。

(1) A. 512×16 bit　　B. 256×8 bit　　C. 256×16 bit　　D. 1024×8 bit

● 若某计算机系统由两个部件串联构成，其中一个部件的失效率为 7×10^{-6}/小时。若不考虑其他因素的影响，并要求计算机系统的平均故障间隔时间为 10^5 小时，则另一个部件的失效率应为 (2) /小时。

(2) A. 2×10^{-5}　　B. 3×10^{-5}　　C. 4×10^{-6}　　D. 3×10^{-6}

● 在 CPU 与主存之间设置高速缓冲器 Cache，其目的是 (3) 。

(3) A. 扩大主存的存储容量　　B. 提高 CPU 对主存的访问效率
C. 既扩大主存容量又提高存取速度　　D. 提高外存储器的存取速度

● 内聚性和耦合性是度量软件模块独立性的重要标准，软件设计时应力求 (4) 。

(4) A. 高内聚，高耦合　　B. 高内聚，低耦合
C. 低内聚，高耦合　　D. 低内聚，低耦合

● 若文件系统容许不同用户的文件可以具有相同的文件名，则操作系统应采用 (5) 来实现。

(5) A. 索引表　　B. 索引文件　　C. 指针　　D. 多级目录

● 结构化开发方法中，数据流图是 (6) 阶段产生的成果。

(6) A. 需求分析　B. 总体设计　C. 详细设计　D. 程序编码

● 某系统的进程状态转换如图 14.1 所示，图中 1、2、3、4 分别表示引起状态转换的不同原因，原因 4 表示 (7) 。

(7) A. 就绪进程被调度　B. 运行进程执行了 P 操作
C. 发生了阻塞进程等待的事件　D. 运行进程时间片到了

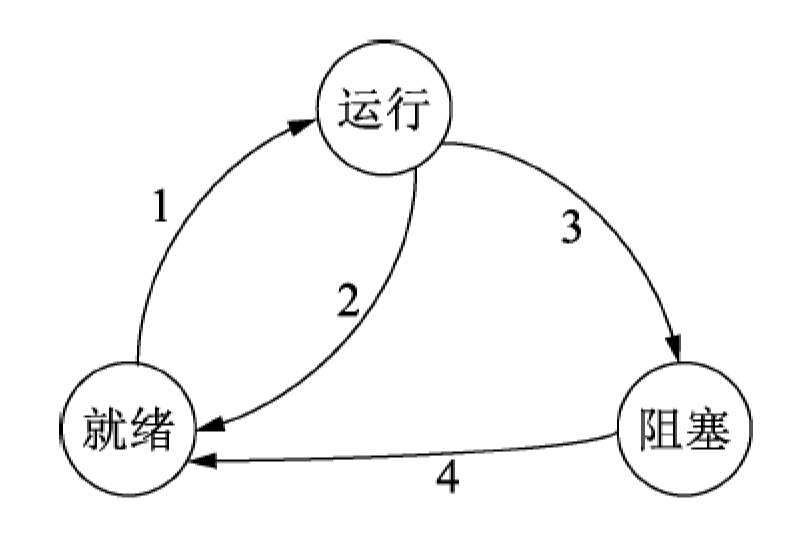


图 14.1　进程状态转换

● 在面向对象的软件工程中，一个组件(Component)包含了 (8) 。

(8) A. 所有的属性和操作　B. 各个类的实例
C. 每个演员(Device or User)的作用　D. 一些协作的类的集合

● 在软件项目管理中可以使用各种图形工具来辅助决策，下面对 Gantt 图的描述中，不正确的是 (9) 。

(9) A. Gantt 图表现了各个活动的持续时间
B. Gantt 图表现了各个活动的起始时间
C. Gantt 图反映了各个活动之间的依赖关系
D. Gantt 图表现了完成各个活动的进度

● 如果两名以上的申请人分别就同样的发明创造申请专利，专利权应授予 (10) 。

(10) A. 最先发明的人　B. 最先申请的人
C. 所有申请人　D. 协商后的申请人

● 设信道带宽为 4000 Hz，调制为 4 种不同的码元，根据 Nyquist 定理，理想信道的数据速率为 (11) 。

(11) A. 10 Kb/s　B. 16 Kb/s　C. 24 Kb/s　D. 48 Kb/s

● 与多模光纤相比较，单模光纤具有 (12) 等特点。

(12) A. 较高的传输率、较长的传输距离、较高的成本
B. 较低的传输率、较短的传输距离、较高的成本
C. 较高的传输率、较短的传输距离、较低的成本
D. 较低的传输率、较长的传输距离、较低的成本

● 关于曼彻斯特编码，下面叙述中错误的是 (13) 。

(13) A. 曼彻斯特编码是一种双相码
B. 采用曼彻斯特编码，波特率是数据速率的 2 倍
C. 曼彻斯特编码可以自同步
D. 曼彻斯特编码效率高

● 下面关于 DPSK 调制技术的描述，正确的是 (14) 。



(14) A. 不同的码元幅度不同　　B. 不同的码元前沿有不同的相位改变
C. 由 4 种相位不同的码元组成　　D. 由不同的频率组成不同的码元

● E1 信道的数据频率是__(15)__，其中的每个话音信道的数据速率是__(16)__。

(15) A. 1.554 Mb/s　B. 2.048 Mb/s　C. 6.312 Mb/s　D. 44.736 Mb/s

(16) A. 56 Kb/s　B. 64 Kb/s　C. 128 Kb/s　D. 2048 Kb/s

● 8 个 9600 b/s 的信道按时分多路复用在一条线路上传输，在统计 TDM 情况下，假定每个子信道有 80%的时间忙，复用线路的控制开销为 5%，那么复用线路的带宽为__(17)__。

(17) A. 32 Kb/s　B. 64 Kb/s　C. 72 Kb/s　D. 96 Kb/s

● 使用海明码进行纠错，7 位码长($x_7x_6x_5x_4x_3x_2x_1$)，其中 4 位数据监督关系式为：

$$c_0 = x_1+x_3+x_5+x_7$$
$$c_1 = x_2+x_3+x_6+x_7$$
$$c_2 = x_4+x_5+x_6+x_7$$

如果接收到的码字为 1000101，那么纠错后的码字是__(18)__。

(18) A. 1000001　B. 1000101　C. 1001101　D. 1010101

● 使用 ADSL 拨号上网，需要在用户端安装__(19)__协议。

(19) A. PPP　B. SLIP　C. PPTP　D. PPPoE

● 在 X.25 网络中，__(20)__是网络层协议。

(20) A. LAP-B　B. X.21　C. X.25 PLP　D. MHS

● 关于路由器，下列说法中错误的是__(21)__。

(21) A. 路由器可以隔离子网，抑制广播风暴
B. 路由器可以实现网络地址转换
C. 路由器可以提供可靠性不同的多条路由选择
D. 路由器只能实现点对点的传输

● 下面关于 ICMP 协议的描述中，正确的是__(22)__。

(22) A. ICMP 协议根据 MAC 地址查找对应的 IP 地址
B. ICMP 协议把公网的 IP 地址转换为私网的 IP 地址
C. ICMP 协议根据网络通信的情况把控制报文传送给发送方主机
D. ICMP 协议集中管理网络中的 IP 地址分配

● TCP 段头的最小长度是__(23)__字节。

(23) A. 16　B. 20　C. 24　D. 32

● 下面信息中__(24)__包含在 TCP 头中而不包含在 UDP 头中。

(24) A. 目标端口号　B. 顺序号　C. 发送端口号　D. 校验和

● ARP 协议的作用是__(25)__，ARP 报文封装在__(26)__中传送。

(25) A. 由 IP 地址查找对应的 MAC 地址
B. 由 MAC 地址查找对应的 IP 地址
C. 由 IP 地址查找对应的端口号
D. 由 MAC 地址查找对应的端口号

(26) A. 以太帧　B. IP 数据报　C. UDP 报文　D. TCP 报文

● 关于 OSPF 协议，下列说法错误的是__(27)__。

(27) A. OSPF 的每个区域(Area)是运行路由选择算法的一个实例
B. OSPF 路由器向各个活动端口组播 Hello 分组来发现邻居路由器
C. Hello 协议还用来选择指定路由器，每个区域选出一个指定路由器
D. OSPF 协议默认的路由更新周期为 30 秒

● 关于链路状态协议与距离矢量协议的区别，以下说法中错误的是 (28) 。

(28) A. 链路状态协议周期性地发布路由信息，而距离矢量协议在网络拓扑发生变化时发布路由信息
B. 链路状态协议由网络内部指定的路由器发布路由信息，而距离矢量协议的所有路由器都发布路由信息
C. 链路状态协议采用组播方式发布路由信息，而距离矢量协议以广播方式发布路由信息
D. 链路状态协议发布的组播报文要求应答，这种通信方式比不要求应答的广播通信可靠

● 以下关于 FTP 和 TFTP 的描述中，正确的是 (29) 。

(29) A. FTP 和 TFTP 都基于 TCP 协议
B. FTP 和 TFTP 都基于 UDP 协议
C. FTP 基于 TCP 协议，TFTP 基于 UDP 协议
D. FTP 基于 UDP 协议，TFTP 基于 TCP 协议

● <title style="italic">science</title>是一个 XML 元素的定义，其中元素标记的属性值是 (30) 。

(30) A. title　　B. style　　C. italic　　D. science

● 在 FTP 协议中，控制连接是由 (31) 主动建立的。

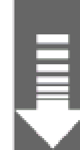
(31) A. 服务器端　　B. 客户端　　C. 操作系统　　D. 服务提供商

● 关于交换机，下面说法中错误的是 (32) 。

(32) A. 以太网交换机根据 MAC 地址进行交换
B. 帧中继交换机根据虚电路号 DLCI 进行交换
C. 三层交换机根据网络层地址进行转发，并根据 MAC 地址进行交换
D. ATM 交换机根据虚电路标识和 MAC 地址进行交换

● 下面是显示交换机端口状态的例子。

```
2950# show interface fastEthernet0/1 switchport
Name: fa0/1
Switchport: Enabled
Administrative mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot 1q
Operational Trunking Encapsulation: dot 1q
Negotiation of Trunking: Disabled
Access Mode VLAN:0 ((Inactive))
Trunking Native Mode VLAN: 1(default)
Trunking VLANs Enabled: ALL
Trunking VLANs Active: 1,2
Pruning VLANs Enabled: 2-1001
```



```
Priority for untagged frames:0
Override vlan tag priority: FALSE
Voice VLAN:none
```

在以上显示的信息中，端口 fa0/1 的链路模式被设置为 (33) ，默认的 VLAN 为 (34) 。

(33) A. 中继连接状态，并要求对方也建立中继连接
B. 中继连接状态，不要求与对方建立中继连接
C. 接入链路状态，要求与对方建立中继连接
D. 接入链路状态，不要求对方建立中继连接

(34) A. VLAN0　B. VLAN1　C. VLAN2　D. VLAN3

● 要显示路由器的运行配置，下面的路由器命令中，正确的是 (35) 。

(35) A. R1 # show running-config　B. R1 # show startup-config
C. R1 > show startup-config　D. R1 > show running-config

● 要使 Samba 服务器在网上邻居中出现的主机名为 smbserver，其配置文件 smb.conf 中应包含 (36) 。

(36) A. workgroup=smbserver　B. netbios name=smbserver
C. server string=smbserver　D. guest account=smbserver

● 在 Linux 系统中，利用 (37) 命令可以分页显示文件的内容。

(37) A. list　B. cat　C. more　D. cp

● 某 DHCP 服务器的地址池范围为 192.36.96.101～192.36.96.150，该网段下某 Windows 工作站启动后，自动获得的 IP 地址是 169.254.220.167，这是因为 (38) 。

(38) A. DHCP 服务器提供保留的 IP 地址
B. DHCP 服务器不工作
C. DHCP 服务器设置租约时间太长
D. 工作站接到了网段内其他 DHCP 服务器提供的地址

● 某 Apache 服务器的配置文件 httpd.conf 包含如下所示配置项。在 (39) 处选择合适的选项，使得用户可通过 http://www.test.cn 访问到该 Apache 服务器；当用户访问 http://111.25.4.30:80 时，会访问到 (40) 虚拟主机。

```
NameVirtualHost 111.25.4.30: 80
<VirtualHost 111.25.4.30: 80>
ServerName www.othertest.com
DocumentRoot /www/othertest
</VirtualHost>
<VirtualHost 111.25.4.30: 80>
ServerName (39)
DocumentRoot /www/otherdate
</VirtualHost>
<VirtualHost 111.25.4.30: 80>
ServerName www.test.com
ServerAlias test.com *.test.com
DocumentRoot /www/test
</VirtualHost>
```

(39) A. www.othertest.com　B. www.test.com

C. www.test.cn　　D. ftp.test.com

(40) A. www.othertest.com　　B. www.test.com

C. www.test.cn　　D. ftp.test.com

● 使用代理服务器(Proxy Server)访问 Internet 的主要功能不包括 (41) 。

(41) A. 突破对某些网站的访问限制　　B. 提高访问某些网站的速度

C. 避免来自 Internet 上病毒的入侵　　D. 隐藏本地主机的 IP 地址

● 以下关于 Windows Server 2003 的域管理模式的描述中，正确的是 (42) 。

(42) A. 域间信任关系只能是单向信任

B. 只有一个主域控制器，其他都为备份域控制器

C. 每个域控制器都可以改变目录信息，并把变化的信息复制到其他域控制器上

D. 只有一个域控制器可以改变目录信息

● 在 Windows Server 2003 中，默认情况下 (43) 组用户拥有访问和完全控制终端服务器的权限。

(43) A. Interactive　　B. Network　　C. Everyone　　D. System

● DES 是一种 (44) 算法。

(44) A. 共享密钥　　B. 公开密钥　　C. 报文摘要　　D. 访问控制

● 某 Web 网站向 CA 申请了数字证书。用户登录该网站时，通过验证 (45) ，可确认该数字证书的有效性，从而 (46) 。

(45) A. CA 的签名　　B. 网站的签名　　C. 会话密钥　　D. DES 密码

(46) A. 向网站确认自己的身份　　B. 获取访问网站的权限

C. 和网站进行双向认证　　D. 验证该网站的真伪

● IPSec VPN 安全技术没有用到 (47) 。

(47) A. 隧道技术　　B. 加密技术　　C. 入侵检测技术　　D. 身份认证技术

● 安全电子邮件协议(PGP)不支持 (48) 。

(48) A. 确认发送者的身份　　B. 确认电子邮件未被修改

C. 防止非授权者阅读电子邮件　　D. 压缩电子邮件大小

● 在 Windows XP 中用事件查看器查看日志文件，可看到的日志包括 (49) 。

(49) A. 用户访问日志、安全性日志和系统日志

B. 应用程序日志、安全性日志和系统日志

C. 网络攻击日志、安全性日志和记账日志

D. 网络连接日志、安全性日志和服务日志

● 在 Windows 中运行 (50) 命令后得到如图 14.2 所示的结果，该命令的作用是 (51) 。

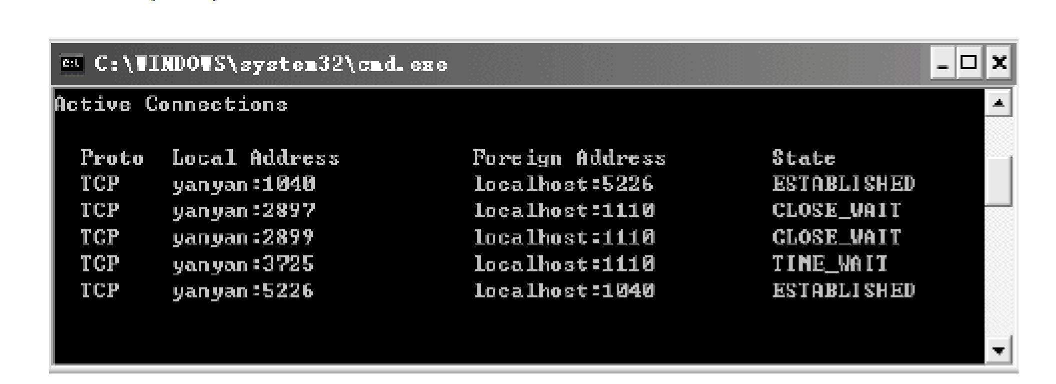
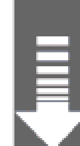


图 14.2　命令运行结果

(50) A. ipconfig /all　　B. ping　　C. netstat　　D. nslookup





(51) A. 查看当前 TCP/IP 配置信息　　　B. 测试与目的主机的连通性
C. 显示当前所有连接及状态信息　　D. 查看当前 DNS 服务器

● 在网络管理中要防范各种安全威胁。在 SNMPv3 中，不必要或无法防范的安全威胁是__(52)__。

(52) A. 篡改管理信息：通过改变传输中的 SNMP 报文实施未经授权的管理操作
B. 通信分析：第三者分析管理实体之间的通信规律，从而获取管理信息
C. 假冒合法用户：未经授权的用户冒充授权用户，企图实施管理操作
D. 消息泄露：SNMP 引擎之间交换的信息被第三者偷听

● 能显示 TCP 和 UDP 连接信息的命令是__(53)__。

(53) A. netstat -s　　B. netstat -e　　C. netstat -r　　D. netstat -a

● 计算机系统中广泛采用了 RAID 技术，在各种 RAID 技术中，磁盘容量利用率最低的是__(54)__。

(54) A. RAID0　　B. RAID1　　C. RAID3　　D. RAID5

● 私网地址用于企业内部 IP 地址分配，网络标准规定的私网地址有__(55)__。

(55) A. A 类有 10 个：10.0.0.0～20.0.0.0
B. B 类有 16 个：172.0.0.0～172.15.0.0
C. C 类有 256 个：192.168.0.0～192.168.255.0
D. D 类有 1 个：244.0.0.0

● 某校园网的地址是 202.100.192.0/18，要把该网络分成 30 个子网，则子网掩码应该是__(56)__，每个子网可分配的主机地址数是__(57)__。

(56) A. 255.255.200.0　　B. 255.255.224.0
C. 255.255.254.0　　D. 255.255.255.0

(57) A. 32　　B. 64　　C. 510　　D. 512

● 分配给某校园网的地址块是 202.105.192.0/18，该校园网包含__(58)__个 C 类网络。

(58) A. 6　　B. 14　　C. 30　　D. 62

● 配置 VLAN 有多种方法，下面选项中不是配置 VLAN 方法的是__(59)__。

(59) A. 把交换机端口指定给某个 VLAN
B. 把 MAC 地址指定给某个 VLAN
C. 由 DHCP 服务器动态地为计算机分配 VLAN
D. 根据上层协议来划分 VLAN

● 可以采用静态或动态方式来划分 VLAN，下面属于静态划分方法的是__(60)__。

(60) A. 按端口划分　　B. 按 MAC 地址划分
C. 按协议类型划分　　D. 按逻辑地址划分

● 在某园区网中，路由器 R1 的 GE0/1(212.112.8.5/30)与路由器 R2 的 GE0/1(212.112.8.6/30)相连，R2 的 GE0/2(212.112.8.13/30)直接与 Internet 上的路由器相连。路由器 R1 默认路由的正确配置是__(61)__。

(61) A. ip route 0.0.0.0 0 0.0.0.0 212.112.8.6
B. ip route 0.0.0.0 0 0.0.0.0 212.112.8.9
C. ip route 0.0.0.0 0 0.0.0.0 212.112.8.10

D. ip route 0.0.0.0 0 0.0.0.0 212.112.8.13

● IEEE 802 局域网中的地址分为两级，其中 LLC 地址是 (62) 。

(62) A. 应用层地址　　B. 上层协议实体的地址
C. 主机的地址　　D. 网卡的地址

● 关于 IEEE 802.3 的 CSMA/CD 协议，下面结论中错误的是 (63) 。

(63) A. CSMA/CD 是一种解决访问冲突的协议
B. CSMA/CD 协议适用于所有 802.3 以太网
C. 在网络负载较小时，CSMA/CD 协议的通信效率很高
D. 这种网络协议适合传播非实时数据

● 以下属于万兆以太网物理层标准的是 (64) 。

(64) A. IEEE 802.3u　　B. IEEE 802.3a　　C. IEEE 802.3e　　D. IEEE 802.3ae

● IEEE 802.11 定义了无线局域网的两种工作模式，其中 (65) 模式是一种点对点连接的网络，不需要无线接入点和有线网络的支持。IEEE 802.11 g 的物理层采用了扩频技术，工作在 (66) 频段。

(65) A. Roaming　　B. Ad Hoc　　C. Infrastructure　　D. Diffuse IP
(66) A. 600 MHz　　B. 800 MHz　　C. 2.4 GHz　　D. 19.2 GHz

● 在建筑群布线子系统所采用的铺设方式中，能够对线缆提供最佳保护的方式是 (67) 。

(67) A. 巷道布线　　B. 架空布线　　C. 直埋布线　　D. 地下管道布线

● 在进行金融业务系统的网络设计时，应该优先考虑 (68) 原则。在进行企业网络的需求分析时，应该首先进行 (69) 。

(68) A. 先进性　　B. 开放性　　C. 经济性　　D. 高可用性
(69) A. 企业应用分析　　B. 网络流量分析
C. 外部通信环境调研　　D. 数据流向图分析

● 层次化网络设计方案中， (70) 是核心层的主要任务。

(70) A. 高速数据转发　　B. 接入 Internet
C. 工作站接入网络　　D. 实现网络的访问策略控制

● NAC's (Network Access Control) role is to restrict network access to only compliant endpoints and (71) users. However, NAC is not a complete LAN (72) solution; additional proactive and (73) security measures must be implemented. Nevis is the first and only comprehensive LAN security solution that combines deep security processing of every packet at 10Gb/s, ensuring a high level of security plus application availability and performance. Nevis integrates NAC as the first line of LAN security (74) . In addition to NAC, enterprises need to implement role-based network access control as critical proactive security measures — real-time, multilevel (75) inspection and microsecond threat containment.

(71) A. automated　　B. distinguished　　C. authenticated　　D. destructed
(72) A. crisis　　B. security　　C. favorable　　D. excellent
(73) A. constructive　　B. reductive　　C. reactive　　D. productive
(74) A. defense　　B. intrusion　　C. inbreak　　D. protection
(75) A. port　　B. connection　　C. threat　　D. insurance



下午科目

试题一(15 分)

阅读以下说明，回答问题 1 至问题 3。

【说明】

某校园网物理地点分布如图 14.3 所示，拓扑结构如图 14.4 所示。

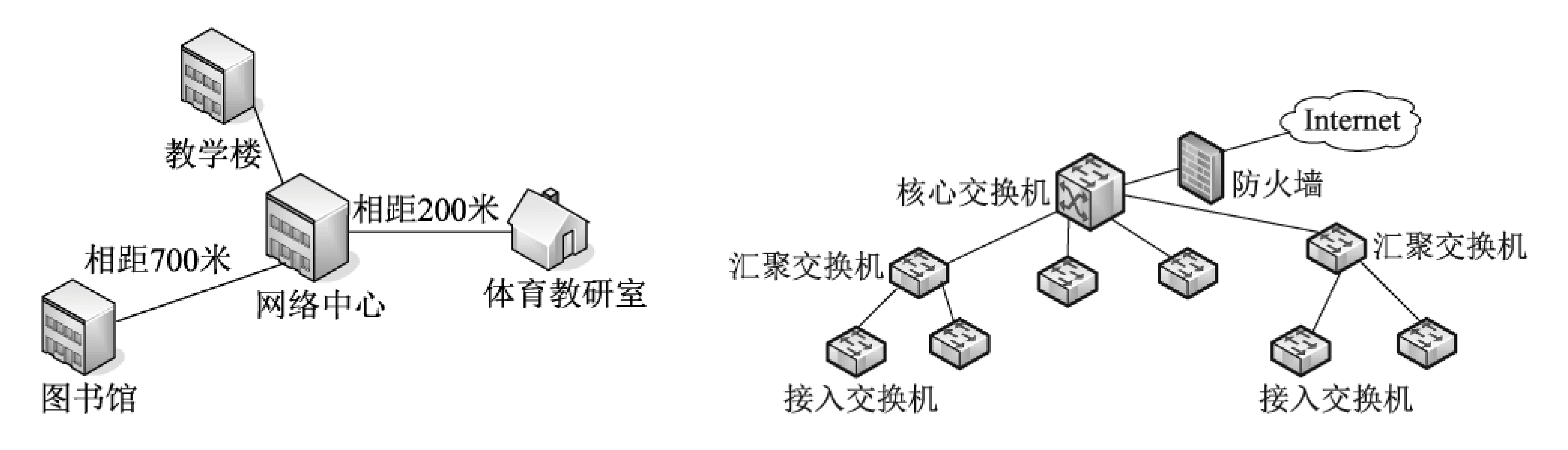


图 14.3　某校园网物理地点分布　　　　图 14.4　网络拓扑结构

【问题 1】(2 分)

由图 14.3 可见，网络中心与图书馆相距 700 米，而且两者之间采用千兆连接，那么两个楼之间的通信介质应选择__(1)__，理由是__(2)__。

(1)备选答案：

A. 单模光纤　　B. 多模光纤　　C. 同轴电缆　　D. 双绞线

【问题 2】(5 分，空(6)为 2 分，其他每空 1 分)

校园网对校内提供 VOD 服务，对外提供 Web 服务，同时进行网络流量监控。对以上服务器进行部署：VOD 服务器部署在__(3)__； Web 服务器部署在__(4)__；网络流量监控服务器部署在__(5)__。

(3)～(5)备选答案：

A. 核心交换机端口　B. 核心交换机镜像端口　C. 汇聚交换机端口

D. 接入交换机端口　E. 防火墙 DMZ 端口

以上 3 种服务器中通常发出数据流量最大的是__(6)__。

【问题 3】(8 分)

校园网在进行 IP 地址部署时，给某基层单位分配了一个 C 类地址块 192.168.110.0/24，该单位的计算机数量分布如表 14.1 所示。要求各部门处于不同的网段，请将表 14.2 中的(7)～(14)处空缺的主机地址(或范围)和子网掩码填写在答题纸的相应位置。

表 14.1　计算机数量分布

部　门	主机数量/台
教师机房	100
教研室 A	32
教研室 B	20
教研室 C	25

表 14.2 地址范围和子网掩码

部　门	可分配的地址范围	子网掩码
教师机房	192.168.110.1～(7)	(11)
教研室 A	(8)	(12)
教研室 B	(9)	(13)
教研室 C	(10)	(14)

试题二(15 分)

阅读以下说明，回答问题 1 至问题 6。

【说明】

某公司要在 Windows Server 2003 上搭建内部 FTP 服务器，服务器分配有一个静态的公网 IP 地址 200.115.12.3。

【问题 1】(每空 2 分，共 4 分)

在控制面板的“添加/删除程序”对话框中选择__(1)__，在打开的“Windows 组件”对话框中选中“应用程序服务器”复选框，然后单击“详细信息”按钮，打开“应用程序服务器”对话框，在__(2)__选项组选中“文件传输协议(FTP)服务”复选框，就可以在 Windows Server 2003 中安装 FTP 服务。

备选答案：

(1) A. 更改或删除程序　　B. 添加新程序
　　C. 添加/删除 Windows 组件　　D. 设定程序访问和默认值

(2) A. ASP.NET　　B. Internet 信息服务(IIS)
　　C. 应用程序服务器控制台　　D. 启用网络服务

【问题 2】(2 分)

安装完 FTP 服务后，系统建立了一个使用默认端口的“默认 FTP 站点”，若要新建另一个使用用户隔离模式的 FTP 站点“内部 FTP 站点”，为了使两个 FTP 服务器不产生冲突，在图 14.5 所示的“内部 FTP 站点”属性对话框中的 IP 地址应配置为__(3)__，端口号应配置为__(4)__。

备选答案：

(3) A. 127.0.0.1　　B. 200.115.12.3　　C. 200.115.12.4　　D. 192.168.0.0

(4) A. 20　　B. 21
　　C. 80　　D. 服务器 1024～65535 中未用端口号

【问题 3】(2 分)

在图 14.6 中，新建 FTP 站点的默认主目录为__(5)__。

备选答案：

(5) A. C:\inetpub\ftproot　　B. C:\ftp
　　C. C:\ftp\root　　D. C:\inetpub\wwwroot




图 14.5　FTP 站点创建向导

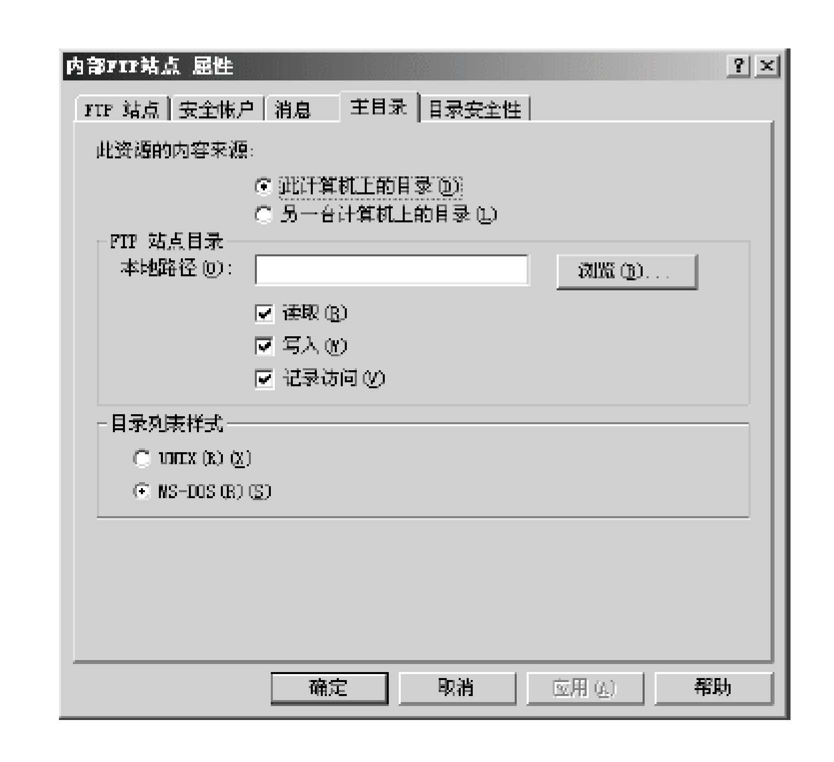


图 14.6　内部 FTP 站点属性

【问题 4】(每空 2 分，共 4 分)

公司要为每个员工在服务器上分配一个不同的 FTP 访问目录，且每个用户只能访问自己目录中的内容，需要进行以下操作：__(6)__ 和 __(7)__。

备选答案：

(6)　A. 为每个员工分别创建一个 Windows 用户

　　B. 在“内部 FTP 站点”中为每个员工分别创建一个用户

　　C. 为每个员工分别设置一个用户名和密码

(7)　A. 在主目录下为每个用户创建一个与用户名相同的子目录

　　B. 在主目录下的 Local User 子目录中为每个用户创建一个与用户名相同的子目录

　　C. 在主目录下的 Local User 子目录中为每个用户创建一个子目录，并在 FTP 中设置为用户可访问

　　D. 在主目录下为每个用户创建一个与用户名相同的虚拟目录

【问题 5】(1 分)

如果还要为其他用户设置匿名登录访问，需要在以上创建用户目录的同一目录下创建名为 __(8)__ 的目录。

备选答案：

(8)　A. iUser　　B. users　　C. public　　D. anonymous

【问题 6】(2 分)

如果公司只允许 IP 地址段 200.115.12.0/25 上的用户访问“内部 FTP 站点”，应进行如下配置。

在图 14.7 所示的对话框中：

1. 选中 __(9)__ 单选按钮；

2. 单击“添加”按钮，打开图 14.8 所示的对话框。

在图 14.8 所示的对话框中：

1. 选中“一组计算机”单选按钮；

2. 在“IP 地址”文本框中输入地址 __(10)__，在“子网掩码”文本框中输入 255.255.255.128；

3. 单击“确定”按钮结束配置。



图 14.7　目录安全性



图 14.8　授权访问

试题三(15 分)

阅读以下 Linux 系统中关于 IP 地址和主机名转换的说明，回答问题 1 至问题 3。

【说明】

计算机用户通常使用主机名来访问网络中的节点，而采用 TCP/IP 协议的网络是以 IP 地址来标记网络节点的，因此需要一种将主机名转换为 IP 地址的机制。在 Linux 系统中，可以使用多种技术来实现主机名和 IP 地址的转换。

【问题 1】(6 分)

请选择恰当的内容填写在(1)、(2)、(3)空白处。

一般用 Host 表、网络信息服务系统(NIS)和域名服务(DNS)等多种技术来实现主机名和 IP 地址之间的转换。Host 表是简单的文本文件，而 DNS 是应用最广泛的主机名和 IP 地址的转换机制，它使用<u>(1)</u>来处理网络中成千上万个主机和 IP 地址的转换。在 Linux 中，DNS 是由 BIND 软件来实现的。BIND 是一个<u>(2)</u>系统，其中的 resolver 程序负责产生域名信息的查询，一个称为<u>(3)</u>的守护进程，负责回答查询，这个过程称为域名解析。

(1)　A. 集中式数据库　　B. 分布式数据库

(2)　A. C/S　　B. B/S

(3)　A. named　　B. bind　　C. nameserver

【问题 2】(3 分)

图 14.9 是采用 DNS 将主机名解析成一个 IP 地址过程的流程图。请选择恰当的内容填写在(4)、(5)、(6)空白处。

A. 产生一个指定下一域名服务器的响应，送给 DNS 客户

B. 把名字请求转送给下一个域名服务器，进行递归求解，结果返回给 DNS 客户

C. 将查询报文发往某域名服务器

D. 利用 Host 表查询

E. 查询失败

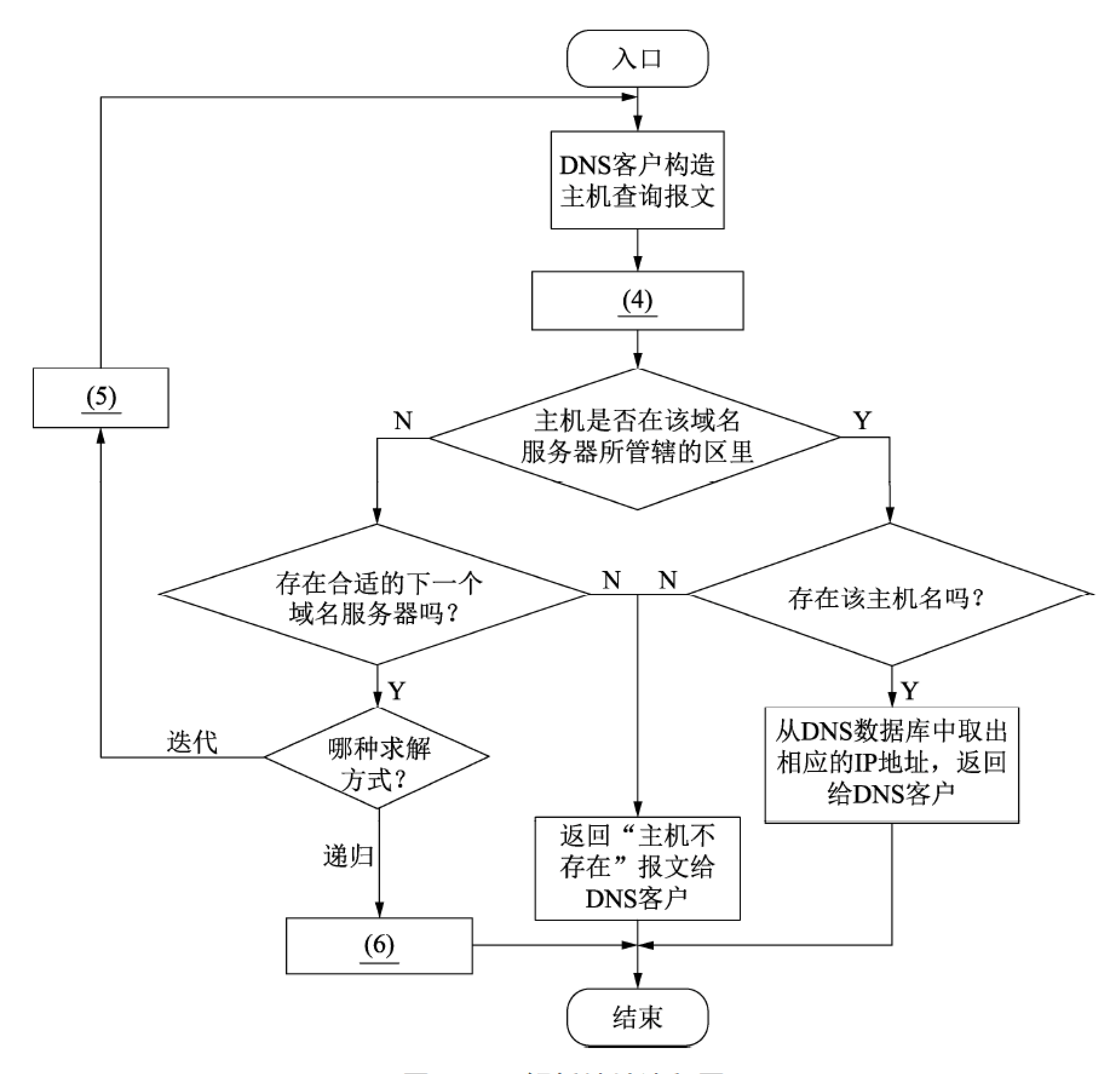


图 14.9　解析地址流程图

【问题 3】(6 分)

请在(7)、(8)、(9)处填写恰当的内容。

在 Linux 系统中设置域名解析服务器，已知该域名服务器上文件 named.conf 的部分内容如下。

```
options {
      directory '/var/named';
   };
   zone '.' {
       type hint;
       file 'named.ca';
   }
   zone 'localhost' IN {
       file "localhost.zone"
       allow-update{none;};
   };
   zone '0.0.127.in-addr.arpa'{
       type master;
       file 'named.local';
   };
   zone 'test.com'{
       type _(7)_;
       file 'test.com';
   };
   zone '40.35.222.in-addr.arpa'{
```

```
        type master;
        file '40.35.222';
    };
    include "/etc/rndc.key";
```

该服务器是域 test.com 的主服务器，该域对应的网络地址是__(8)__，正向域名转换数据文件存放在__(9)__目录中。

试题四(15 分)

阅读以下说明，回答问题 1 至问题 4。

【说明】

网络工程师经常会面对服务器性能不足的问题，尤其是网络系统中的核心资源服务器，其数据流量和计算强度之大，使得单一计算机无法承担。可以部署多台 Linux 服务器组成服务器集群，采用负载均衡技术提供服务。

某企业内部网(网络域名为 test.com)由 3 台 Linux 服务器提供服务，其中 DNS、FTP、SMTP 和 POP3 4 种服务由一台服务器承担，Web 服务由两台 Linux 服务器采用负载均衡技术承担。

【问题 1】(2 分)

假定提供 Web 服务的两台 Linux 服务器的 IP 地址分别为 192.168.1.10 和 192.168.1.20。为了使用 DNS 循环机制，由主机 www.test.com 对外提供一致的服务，需要在 DNS 服务器的 test.com 区域文件中增加下列内容。

```
www1  IN  (1)   192.168.1.10
www2  IN  (1)   192.168.1.20
www   IN  (2)   www1
www   IN  (2)   www2
```

通过 DNS 的循环机制，客户访问主机 www.test.com 时，会依次访问 IP 地址为 192.168.1.10 和 192.168.1.20 的 www 主机。填写上面的空格，完成 test.com 文件的配置。

【问题 2】(2 分)

采用循环 DNS 配置可以实现简单的具有负载均衡功能的 Web 服务。说明采用循环 DNS 实现均衡负载存在什么问题。

【问题 3】(6 分)

图 14.10 所示的是基于硬件的负载均衡方案，其中 WSD Pro 被称为导向器，通过导向器的调度，实现服务的负载均衡。主机 www1.test.com、www2.test.com、www.test.com 和 WSD Pro 都配置了双网卡，IP 地址标注在图 14.10 中。

图中的各个服务器必须进行恰当的配置，主机 ns.test.com 的/etc/sysconfig/network 文件和/etc/sysconfig/ network-scripts/ifcfg-eth0 文件配置如下。

/etc/sysconfig/network 文件清单：

```
NETWORKING=yes
FORWARD_IPV4= (3)
HOSTNAME=ns.test.com
DOMAINNAME=(4)
GATEWAY=(5)
GATEWAYDEV=eth0
```



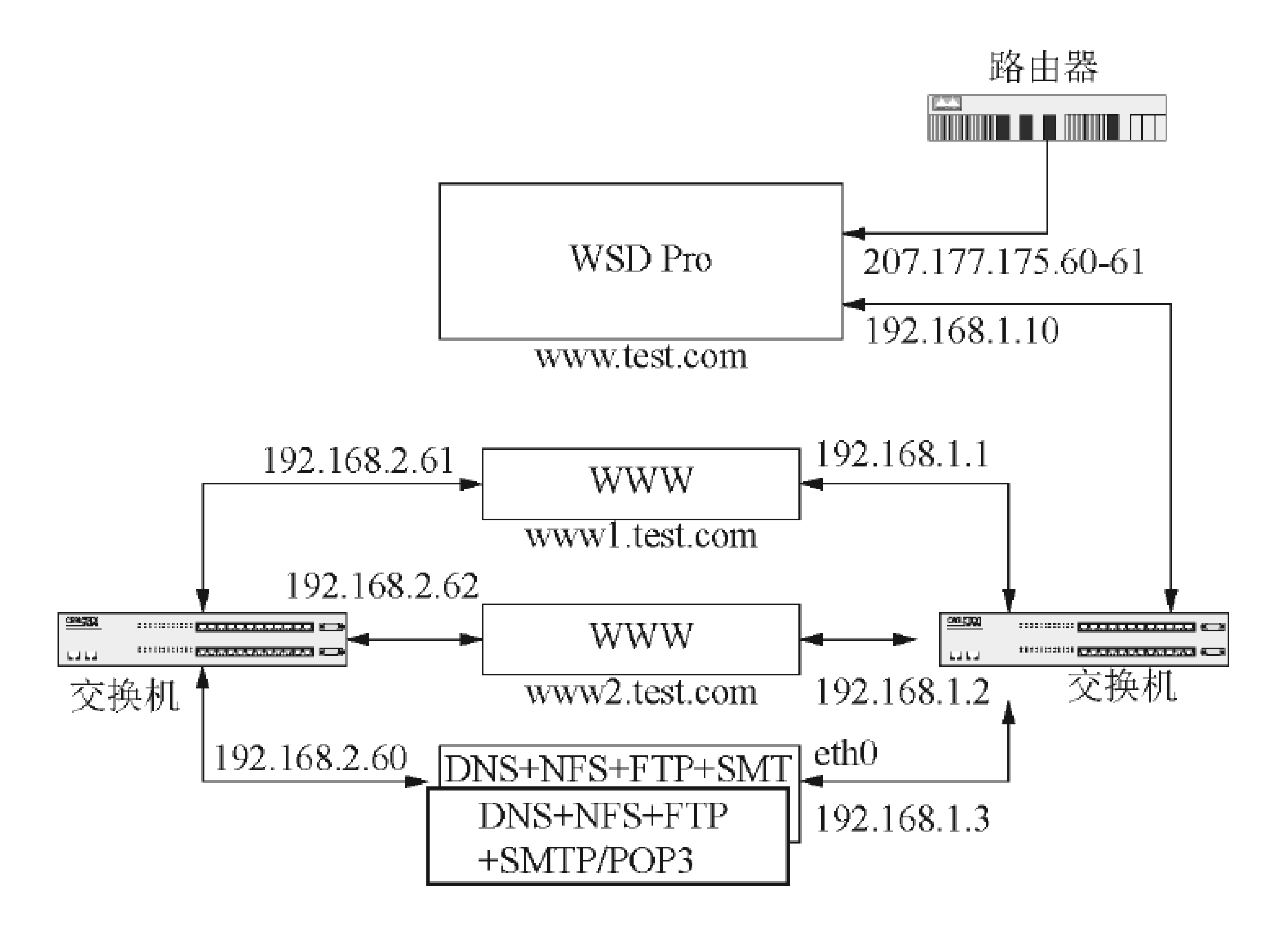


图 14.10　基于硬件的负载均衡方案

/etc/sysconfig/network-scripts/ifcfg-eth0 文件清单：

```
DEVICE=eth0
IPADDR= (6)
NETMASK=255.255.255.0
NETWORK= (7)
BROADCAST=(8)
ONBOOT=yes
```

填写上面的空格，完成文件的配置。

【问题 4】(5 分)

图中所示案例采用 NFS(网络文件系统)技术主要解决什么问题？由图中左边的交换机组成的局域网有何功能？

试题五(15 分)

阅读以下说明，回答问题 1 至问题 4。

【说明】

图 14.11 是 VLAN 配置的结构示意图。

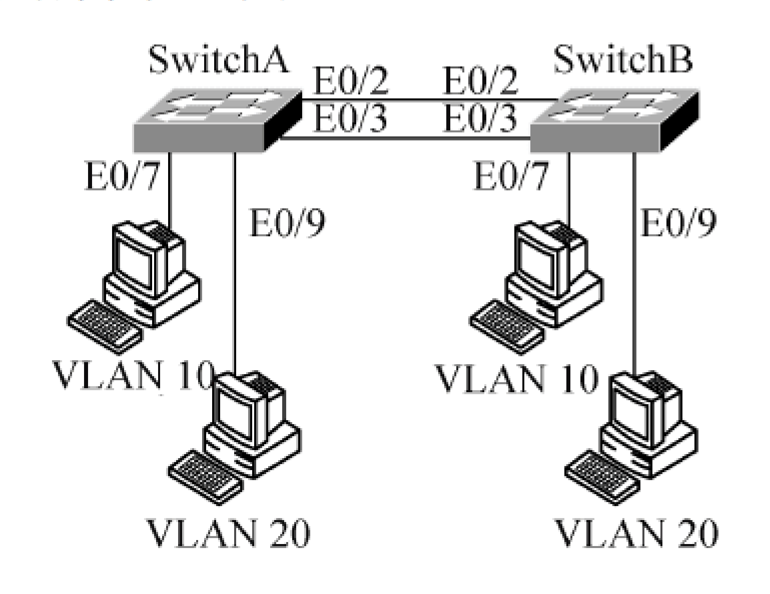


图 14.11　VLAN 配置的结构示意图

【问题 1】(5 分)

请阅读下列 SwitchA 的配置信息，并在(1)～(5)处解释该语句的作用。

```
Switch>enable                                    (进入特权模式)
Switch#config terminal                           (进入配置模式)
Switch(config)#hostname SwitchA                   (1)
SwitchA(config)#end
SwitchA #
SwitchA #vlan database                            (2)
SwitchA (vlan)#vtp server                         (3)
SwitchA (vlan)#vtp domain vtpserver               (4)
SwitchA (vlan)#vtp pruning                        (5)
SwitchA (vlan)#exit                              (退出 VLAN 配置模式)
```

【问题2】(4分)

下面是交换机完成Trunk的部分配置，请根据题目要求，完成下列配置。

```
SwitchA (config)#interface f0/3                          (进入端口 3 配置模式)
SwitchA (config-if)#switchport  (6)                      (设置当前端口为 Trunk 模式)
SwitchA (config-if)# switchport trunk allowed  (7)  (设置允许所有 VLAN 通过)
SwitchA (config-if)#exit
SwitchA (config)#exit
Switch#
```

【问题3】(4分)

```
Switch (config)#interface f0/7                           (进入端口 7 的配置模式)
Switch (config-if)#   (8)                                (设置端口为静态 VLAN 访问模式)
Switch (config-if)#   (9)                                (把端口 7 分配给 VLAN10)
Switch (config-if)#exit
Switch (config)#exit
```

【问题4】(2分)

下面是基于端口权值的负载均衡配置过程。

```
SwitchA (config)#interface f0/2                          (进入端口 2 配置模式)
SwitchA (config-if)#spanning-tree vlan 10 port-priority 10
                                                         (将 VLAN10 的端口权值设为 10)
SwitchA (config-if)#exit
SwitchA (config)#interface f0/3                          (进入端口 3 配置模式)
SwitchA (config-if)#spanning-tree vlan 20 port-priority 10
                                                         (将 VLAN20 的端口权值设为 10)
Switch1 (config-if)#end
Switch1#copy running-config startup-config               (保存配置文件)
```

1. 不同Trunk上不同VLAN的权值不同，在默认情况下，其权值为 (10) 。
2. 按照上述配置，VLAN20的数据通过SwitchA的 (11) 口发送和接收数据。

14.1.2 考前模拟卷 2

上午科目

● 若每一条指令都可以分解为取指、分析和执行3步。已知取指时间 $t_{取指}=4\Delta t$，分析时间 $t_{分析}=3\Delta t$，执行时间 $t_{执行}=5\Delta t$。如果按串行方式执行完100条指令需要 (1) Δt。如果按照流水方式执行，执行完100条指令需要 (2) Δt。

(1) A. 1190　　B. 1195　　C. 1200　　D. 1205





(2)　A. 504　　B. 507　　C. 508　　D. 510

● 页式虚拟存储系统的逻辑地址是由页号和页内地址两部分组成，地址变换过程如图 14.12 所示。假定页面的大小为 8 KB，图 14.12 中所示的十进制逻辑地址 9612 经过地址变换后，形成的物理地址 a 应为十进制__(3)__。

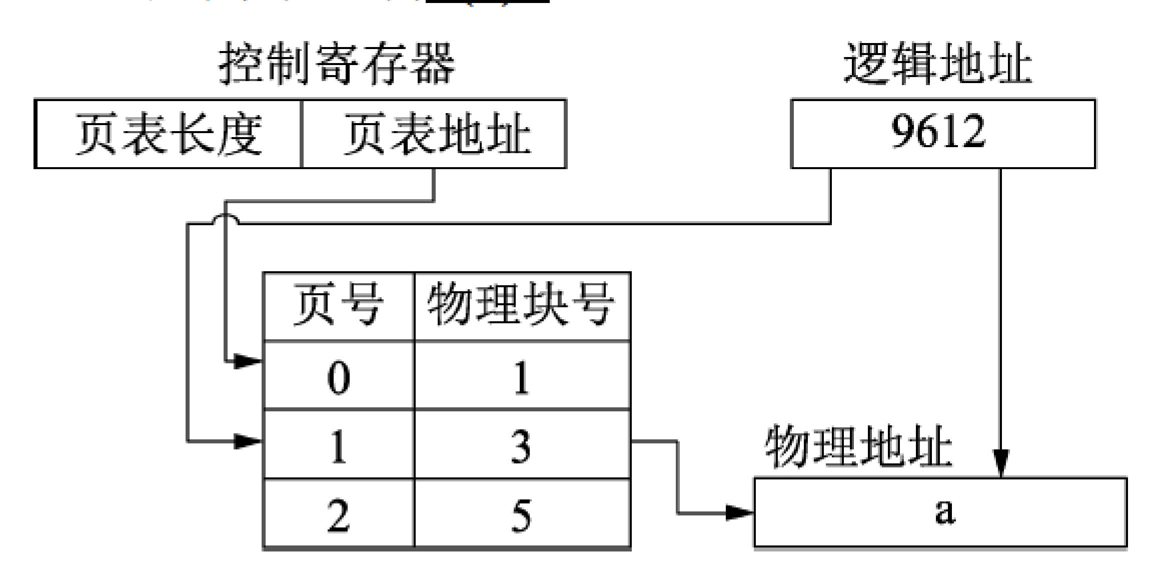


图 14.12　地址变换过程

(3)　A. 42 380　　B. 25 996　　C. 9612　　D. 8192

● __(4)__不属于计算机控制器的部件。

(4)　A. 指令寄存器(IR)　　B. 程序计数器(PC)

C. 算术逻辑单元(ALU)　　D. 程序状态寄存器(PSW)

● 某系统的可靠性结构框图如图 14.13 所示。该系统由 4 个部件组成，其中 2、3 两部件并联冗余，再与 1、4 部件串联构成。假设部件 1、2、3 的可靠度分别为 0.90、0.70、0.70。若要求该系统的可靠度不低于 0.75，则进行系统设计时，分配给部件 4 的可靠度至少应为__(5)__。

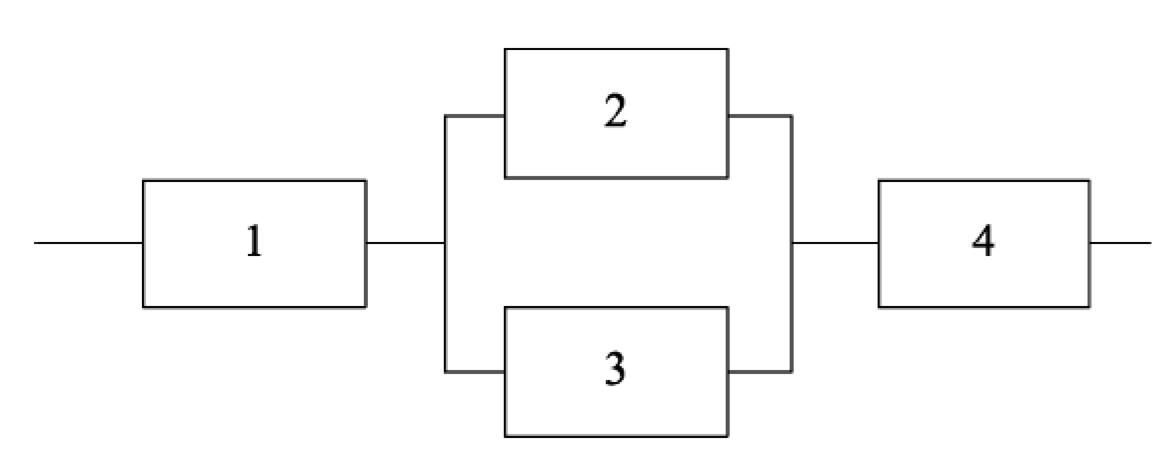


图 14.13　可靠性结构框图

(5)　A. $\dfrac{0.75}{0.9\times(1-0.7)^2}$　　B. $\dfrac{0.75}{0.9\times(1-0.7\times0.7)^2}$

C. $\dfrac{0.75}{0.9\times[1-(1-0.7)^2]}$　　D. $\dfrac{0.75}{0.9\times(0.7+0.7)^2}$

● 关于原型化开发方法的叙述中，不正确的是__(6)__。

(6)　A. 原型化方法适用于需求不明确的软件开发

B. 在开发过程中，可以废弃不用早期构造的软件原型

C. 原型化方法可以直接开发出最终产品

D. 原型化方法利于确认各项系统服务的可用性

● CMM 模型将软件过程的成熟度分为 5 个等级。在__(7)__使用定量分析来不断地改进和管理软件过程。

(7)　A. 优化级　　B. 管理级　　C. 定义级　　D. 可重复级

● 选择软件开发工具时，应考虑功能、 (8) 、稳健性、硬件要求和性能、服务和支持。

(8) A. 易用性　　B. 易维护性　　C. 可移植性　　D. 可扩充性

● 某网络工程计划图如图 14.14 所示，边上的标记为任务编码及其需要的完成时间(天)，则整个工程的工期为 (9) 。

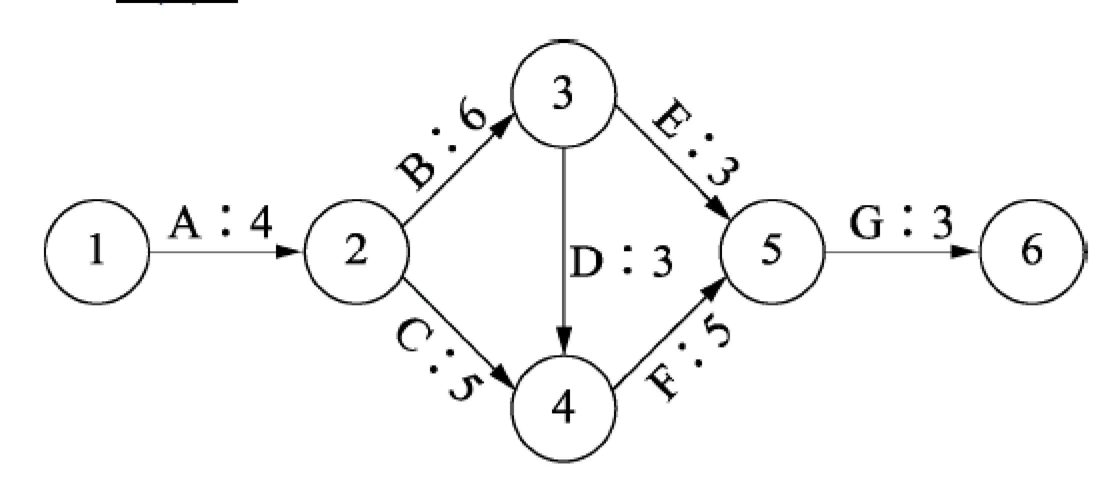


图 14.14　网络工程计划图

(9) A. 16　　B. 17　　C. 18　　D. 21

● 若某人持有盗版软件，但他本人确实不知道该软件是盗版的，则 (10) 承担侵权责任。

(10) A. 应由该软件的持有者
B. 应由该软件的提供者
C. 应由该软件的提供者和持有者共同
D. 该软件的提供者和持有者都不

● 设信道带宽为 4 kHz，采用 4 相调制技术，则信道支持的最大数据率是 (11) 。

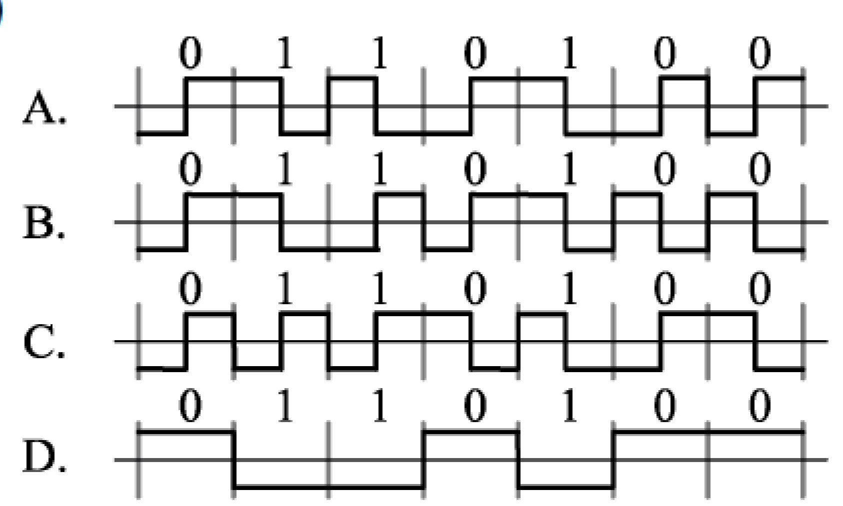
(11) A. 4 Kb/s　　B. 8 Kb/s　　C. 16 Kb/s　　D. 32 Kb/s

● 关于多模光纤，下面的描述中错误的是 (12) 。

(12) A. 多模光纤的芯线由透明的玻璃或塑料制成
B. 多模光纤包层的折射率比芯线的折射率低
C. 光波在芯线中以多种反射路径传播
D. 多模光纤的数据速率比单模光纤的数据速率高

● 下面 4 种编码方式中属于差分曼彻斯特编码的是 (13) 。

(13)



● 在异步通信中，每个字符包括 1 位起始位、7 位数据位、1 位奇偶校验位和 1 位终止位，每秒钟传送 100 个字符，则有效数据速率为 (14) 。

(14) A. 500 b/s　　B. 600 b/s　　C. 700 b/s　　D. 800 b/s

● 在光纤通信标准中，OC-3 的数据速率是 (15) 。

(15) A. 51 Mb/s　　B. 155 Mb/s　　C. 622 Mb/s　　D. 2488 Mb/s



● 在 E1 载波中，每个子信道的数据速率是__(16)__，E1 载波的控制开销占__(17)__。

(16) A. 32 Kb/s　　B. 64 Kb/s　　C. 72 Kb/s　　D. 96 Kb/s

(17) A. 3.125%　　B. 6.25%　　C. 1.25%　　D. 25%

● 若信息码字为 11100011，生成多项式 $G(x) = x^5 + x^4 + x + 1$，则计算出的 CRC 校验码为__(18)__。

(18) A. 01101　　B. 11010　　C. 001101　　D. 0011010

● 以下属于对称数字用户线路(Symmetrical Digital Subscriber Line)的是__(19)__。

(19) A. HDSL　　B. ADSL　　C. RADSL　　D. VDSL

● 下列语句中准确地描述了 ISDN 接口类型的是__(20)__。

(20) A. 基群速率接口(30B+D)中的 D 信道用于传输用户数据和信令，速率为 16 Kb/s

B. 基群速率接口(30B+D)中的 B 信道用于传输用户数据，速率为 64 Kb/s

C. 基本速率接口(2B+D)中的 D 信道用于传输信令，速率为 64 Kb/s

D. 基本速率接口(2B+D)中的 D 信道用于传输用户数据，速率为 16 Kb/s

● 某 IP 网络连接如图 14.15 所示，在这种配置下 IP 全局广播分组不能够通过的路径是__(21)__。

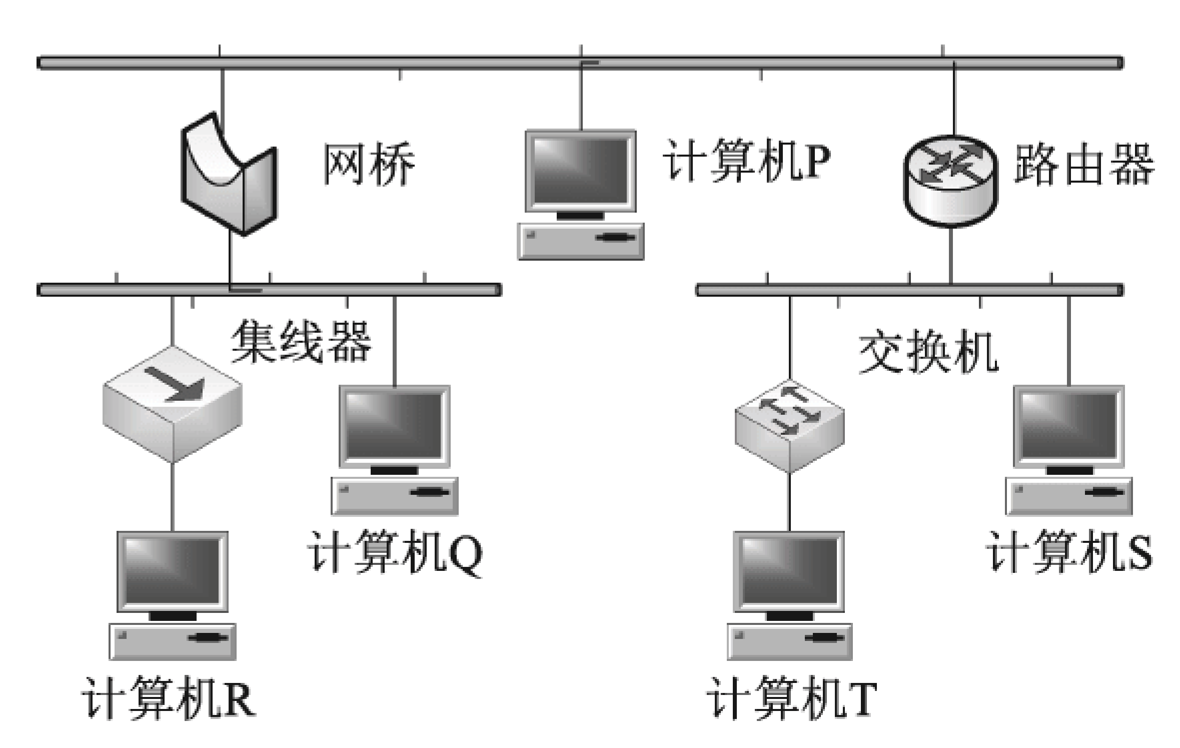


图 14.15　IP 网络连接

(21) A. 计算机 P 和计算机 Q 之间的路径 B. 计算机 P 和计算机 S 之间的路径

C. 计算机 Q 和计算机 R 之间的路径 D. 计算机 S 和计算机 T 之间的路径

● 因特网中的协议应该满足规定的层次关系，下面的选项中能正确表示协议层次和对应关系的是__(22)__。

(22)

A.

SNMP	TFTP
UDP	TCP
IP	

B.

SNMP	HTTP
TCP	UDP
IP	

C.

HTTP	TFTP
TCP	UDP
IP	

D.

SMTP	TELNET
TCP	UDP
IP	

● TCP 是互联网中的传输层协议，使用__(23)__次握手协议建立连接。这种建立连接的方法可以防止__(24)__。

(23) A. 1　　B. 2　　C. 3　　D. 4

(24) A. 出现半连接　　B. 无法连接
C. 产生错误的连接　　D. 连接失败

● 以太网的数据帧封装如图14.16所示，包含在TCP段中的数据部分最长应该是__(25)__字节。

目标MAC地址	源MAC地址	协议类型	IP头	TCP头	数据	CRC

图14.16　以太网的数据帧封装

(25) A. 1434　　B. 1460　　C. 1480　　D. 1500

● 关于ARP表，以下描述中正确的是__(26)__。

(26) A. 提供常用目标地址的快捷方式来减少网络流量
B. 用于建立IP地址到MAC地址的映射
C. 用于在各个子网之间进行路由选择
D. 用于进行应用层信息的转换

● 开放最短路径优先协议(OSPF)采用__(27)__算法计算最佳路由。

(27) A. Dynamic-Search　　B. Bellman-Ford
C. Dijkstra　　D. Spanning-Tree

● 在RIP协议中，可以采用水平分割法(Split Horizon)解决路由环路问题，下面的说法中正确的是__(28)__。

(28) A. 把网络分割成不同的区域以减少路由循环
B. 不要把从一个邻居学习到的路由再发送回该邻居
C. 设置邻居之间的路由度量为无限大
D. 路由器必须把整个路由表发送给自己的邻居

● BGP协议的作用是__(29)__。

(29) A. 用于自治系统之间的路由器间交换路由信息
B. 用于自治系统内部的路由器间交换路由信息
C. 用于主干网中路由器之间交换路由信息
D. 用于园区网中路由器之间交换路由信息

● POP3协议采用__(30)__模式，当客户机需要服务时，客户端软件(Outlook Express或FoxMail)与POP3服务器建立__(31)__连接。

(30) A. Browser/Server　　B. Client/Server
C. Peer to Peer　　D. Peer to Server

(31) A. TCP　　B. UDP　　C. PHP　　D. IP

● 下面的交换机命令中，__(32)__为2950交换机端口指定VLAN。

(32) A. S1(config-if)# vlan-menbership static
B. S1(config-if)# vlan database
C. S1(config-if)# switchport mode access
D. S1(config-if)# switchport access vlan 1

● 关于路由器，下列说法中正确的是__(33)__。

(33) A. 路由器处理的信息量比交换机少，因而转发速度比交换机快

B. 对于同一目标，路由器只提供延迟最小的最佳路由

C. 通常的路由器可以支持多种网络层协议，并提供不同协议之间的分组转换

D. 路由器不但能够根据逻辑地址进行转发，而且可以根据物理地址进行转发

● 配置路由器端口，应该在 (34) 提示符下进行。

(34) A. R1 (config)#　　B. R1 (config-in)#
C. R1 (config-intf)#　　D. R1 (config-if)#

● (35) 能够显示路由器配置了哪种路由协议。

(35) A. R1 (config)# show ip route　　B. R1 > show ip route
C. R1 > show ip protocol　　D. R1 > (config-if)# show ip protocol

● 在 Linux 操作系统中， (36) 文件负责配置 DNS，它包含了主机的域名搜索顺序和 DNS 服务器的地址。

(36) A. /etc/hostname　B. /etc/host.conf　C. /etc/resolv.conf　D. /etc/name.conf

● 在 Linux 系统中，用户组加密后的口令存储在 (37) 文件中。

(37) A. /etc/passwd　B. /etc/shadow　C. /etc/group　D. /etc/shells

● Linux 系统在默认情况下将创建的普通文件的权限设置为 (38) 。

(38) A. -rw-r-r-　B. -r-r-r-　C. -rw-rw-rwx-　D. -rwxrwxrw-

● 活动目录(Active Directory)是由组织单元、域、 (39) 和域林构成的层次结构，安装活动目录要求分区的文件系统为 (40) 。

(39) A. 超域　B. 域树　C. 团体　D. 域控制器

(40) A. FAT16　B. FAT32　C. ext2　D. NTFS

● 在配置 IIS 时，如果想禁止某些 IP 地址访问 Web 服务器，应在“默认 Web 站点”的属性对话框中的“ (41) ”选项卡中进行配置。IIS 的发布目录 (42) 。

(41) A. 目录安全性　B. 文档　C. 主目录　D. ISAPI 筛选器

(42) A. 只能够配置在 c:\inetpub\wwwroot 上
B. 只能够配置在本地磁盘上
C. 只能够配置在联网的其他计算机上
D. 既能够配置在本地的磁盘，也能配置在联网的其他计算机上

● 在 Windows 操作系统中，要实现一台具有多个域名的 Web 服务器，正确的方法是 (43) 。

(43) A. 使用虚拟目录　　B. 使用虚拟主机
C. 安装多套 IIS　　D. 为 IIS 配置多个 Web 服务端口

● 以下用于在网络应用层和传输层之间提供加密方案的协议是 (44) 。

(44) A. PGP　B. SSL　C. IPSec　D. DES

● 包过滤防火墙通过 (45) 来确定数据包是否能通过。

(45) A. 路由表　B. ARP 表　C. NAT 表　D. 过滤规则

● 多形病毒指的是 (46) 的计算机病毒。

(46) A. 可在反病毒检测时隐藏自己　　B. 每次感染都会改变自己
C. 可以通过不同的渠道进行传播　　D. 可以根据不同环境造成不同破坏

● 数据加密标准(DES)是一种分组密码，将明文分成大小 (47) 位的块进行加密，

密钥长度为 (48) 位。

(47) A. 16　B. 32　C. 56　D. 64

(48) A. 16　B. 32　C. 56　D. 64

● SNMP 协议实体发送请求和应答报文的默认端口号是 (49) ，SNMP 代理发送陷入报文(Trap)的默认端口号是 (50) 。

(49) A. 160　B. 161　C. 162　D. 163

(50) A. 160　B. 161　C. 162　D. 163

● 在 Windows 操作系统中，如果要查找从本地出发，经过 3 个跳步，达到名字为 Enric 的目标主机的路径，则输入的命令是 (51) 。

(51) A. tracert Enric-h 3　B. tracert -j 3 Enric
C. tracert -h 3 Enric　D. tracert Enric -j3

● SNMP 采用 UDP 提供数据报服务，这是由于 (52) 。

(52) A. UDP 比 TCP 更加可靠
B. UDP 数据报文可以比 TCP 数据报文大
C. UDP 是面向连接的传输方式
D. 采用 UDP 实现网络管理不会太多增加网络负载

● 嗅探器可以使网络接口处于混杂模式，在这种模式下，网络接口 (53) 。

(53) A. 只能够响应与本地网络接口硬件地址相匹配的数据帧
B. 只能够响应本网段的广播数据帧
C. 只能响应组播信息
D. 能够响应流经网络接口的所有数据帧

● 下面的地址中，属于本地环路地址的是 (54) 。

(54) A. 10.10.10.1　B. 255.255.255.0　C. 127.0.0.1　D. 192.0.0.1

● 局域网中某主机的 IP 地址为 176.16.1.12/20，该局域网的子网掩码为 (55) ，最多可以连接的主机数为 (56) 。

(55) A. 255.255.255.0　B. 255.255.254.0　C. 255.255.252.0　D. 255.255.240.0

(56) A. 4094　B. 2044　C. 1024　D. 512

● 下面的地址中，属于私网地址的是 (57) 。

(57) A. 192.118.10.1　B. 127.1.0.1　C. 172.14.2.240　D. 172.17.20.196

● 一个主机的 IP 地址是 172.16.2.12/24，该主机所属的网络地址是 (58) 。

(58) A. 172.0.0.0　B. 172.16.0.0　C. 172.16.2.0　D. 172.16.1.0

● 设有下面 4 条路由：10.1.193.0/24、10.1.194.0/24、10.1.196.0/24 和 10.1.198.0/24。如果进行路由汇聚，覆盖这 4 条路由的地址是 (59) 。

(59) A. 10.1.192.0/21　B. 10.1.192.0/22　C. 10.1.200.0/22　D. 10.1.224.0/20

● 下列删除 VLAN 的命令中，无法执行的是 (60) 。

(60) A. no vlan 1　B. no vlan 2　C. no vlan 500　D. no vlan 1000

● 下面可以转发不同 VLAN 之间的通信的设备是 (61) 。

(61) A. 二层交换机　B. 三层交换机　C. 网络集线器　D. 生成树网桥

● 下面有关 VLAN 的语句中，正确的是 (62) 。

(62) A. 虚拟局域网中继协议(VLAN Trunk Protocol，VTP)用于在路由器之间交换不同 VLAN 的信息
B. 为了抑制广播风暴，不同的 VLAN 之间必须用网桥分隔
C. 交换机的初始状态是工作在 VTP 服务器模式，这样可以把配置信息广播给其他交换机
D. 一台计算机可以属于多个 VLAN，即它可以访问多个 VLAN，也可以被多个 VLAN 访问

● 以太网的 CSMA/CD 协议采用 1-坚持型监听算法。与其他监听算法相比，这种算法的主要特点是 (63) 。

(63) A. 传输介质利用率低，冲突概率也低
B. 传输介质利用率高，冲突概率也高
C. 传输介质利用率低，但冲突概率高
D. 传输介质利用率高，但冲突概率低

● 快速以太网标准 100Base-TX 采用的传输介质是 (64) 。

(64) A. 同轴电缆　B. 无屏蔽双绞线　C. CATV 电缆　D. 光纤

● 在以太网中，最大传输单元(MTU)是 (65) 字节。

(65) A. 46　B. 64　C. 1500　D. 1518

● 无线局域网标准 IEEE 802.11i 提出了新的 TKIP 协议来解决 (66) 中存在的安全隐患。

(66) A. WAP 协议　B. WEP 协议　C. MD5　D. 无线路由器

● 建立一个家庭无线局域网，使得计算机不但能够连接因特网，而且 WLAN 内部还可以直接通信，正确的组网方案是 (67) 。

(67) A. AP+无线网卡　B. 无线天线+无线 Modem
C. 无线路由器+无线网卡　D. AP+无线路由器

● 网络安全设计是保证网络安全运行的基础，网络安全设计有其基本的设计原则，以下关于网络安全设计原则的描述，错误的是 (68) 。

(68) A. 网络安全的“木桶原则”强调对信息均衡、全面地进行保护
B. 良好的等级划分，是实现网络安全的保障
C. 网络安全系统设计应独立进行，不需要考虑网络结构
D. 网络安全系统应该以不影响系统正常运行为前提

● 园区网络设计中，如果网络需求对 QoS 要求很高，应考虑采用 (69) 网络。

(69) A. ATM　B. 千兆以太　C. FDDI　D. ISDN

● 按照网络分级设计模型，通常把网络设计分为 3 层，即核心层、汇聚层和接入层。以下关于分级网络的描述中，不正确的是 (70) 。

(70) A. 核心层承担访问控制列表检查功能
B. 汇聚层实现网络的访问策略控制
C. 工作组服务器放置在接入层
D. 在接入层可以使用集线器代替交换机

● Originally introduced by Netscape Communications, __(71)__ are a general mechanism which HTTP Server side applications, such as CGI __(72)__, can use to both store and retrieve information on the HTTP __(73)__ side of the connection. Basically, Cookies can be used to compensate for the __(74)__ nature of HTTP. The addition of a simple, persistent, client-side state significantly extends the capabilities of WWW-based __(75)__.

(71) A. Browsers　B. Cookies　C. Connections　D. Scripts
(72) A. graphics　B. processes　C. scripts　D. texts
(73) A. Client　B. Editor　C. Creator　D. Server
(74) A. fixed　B. flexible　C. stable　D. stateless
(75) A. programs　B. applications　C. frameworks　D. constrains

下午科目

试题一(15 分)

阅读以下说明，回答问题 1 至问题 4。

【说明】

某学校计划建立校园网，拓扑结构如图 14.17 所示。该校园网分为核心、汇聚、接入三层，由交换模块、广域网接入模块、远程访问模块和服务器群 4 大部分构成。

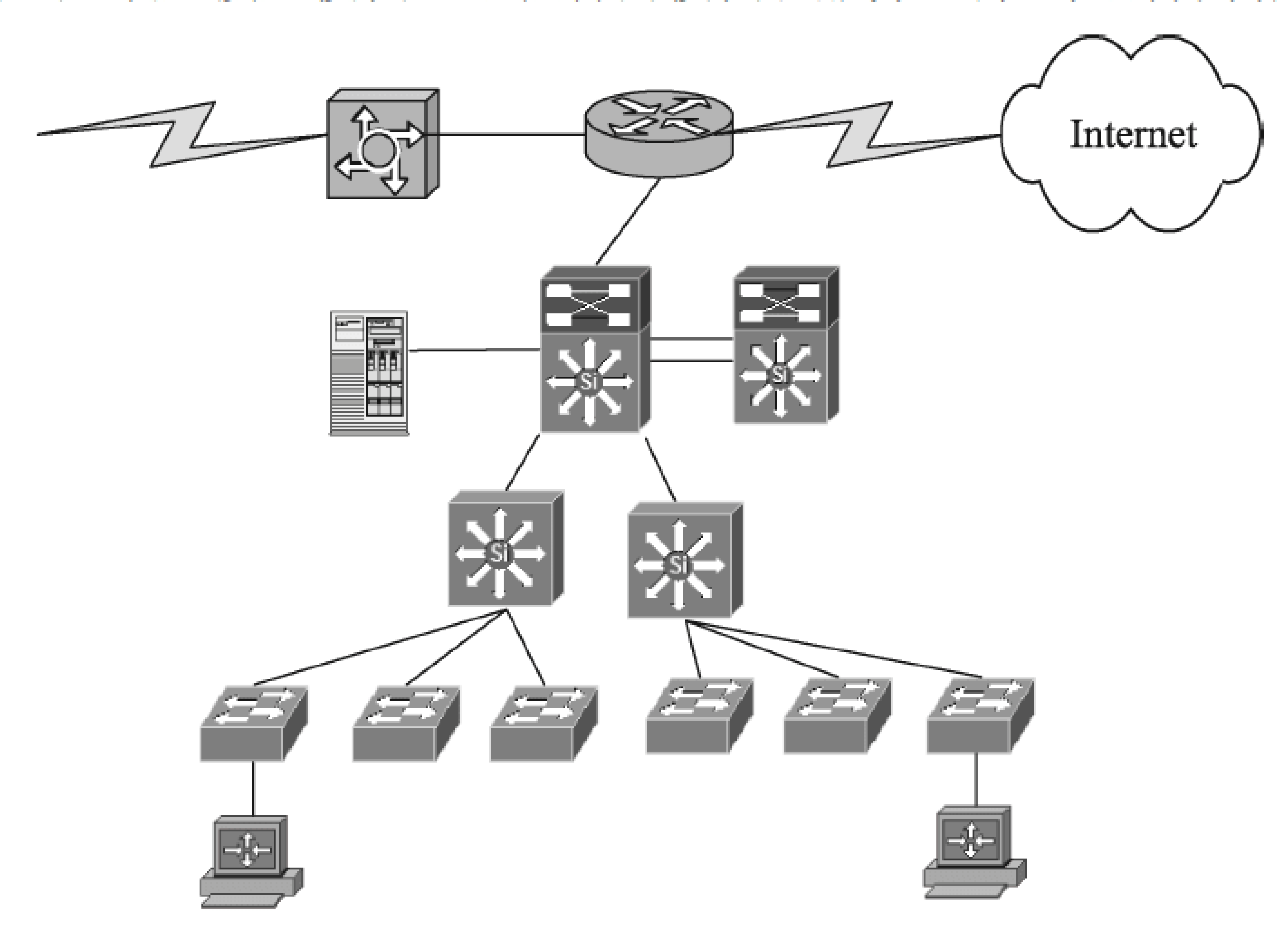


图 14.17　校园网拓扑结构

【问题 1】(5 分)

在校园网设计过程中，划分了很多 VLAN，采用了 VTP 来简化管理。将(1)～(5)处空缺信息填写在对应的位置。

1. VTP 信息只能在__(1)__端口上传播。
2. 运行 VTP 的交换机可以工作在 3 种模式：__(2)__、__(3)__、__(4)__。
3. 共享相同 VLAN 数据库的交换机构成一个__(5)__。

【问题 2】(4 分)

该校园网采用了异步拨号进行远程访问，异步封装协议采用了 PPP 协议。将(6)～(9)处

空缺信息填写在对应的位置。

1. 异步拨号连接属于远程访问中的电路交换服务，远程访问中另外两种可选的服务类型是：__(6)__和__(7)__。

2. PPP 提供了两种可选的身份认证方法，它们分别是__(8)__和__(9)__。

【问题 3】(2 分)

该校园网内交换机数量较多，交换机间链路复杂，为了防止出现环路，需要在各交换机上运行__(10)__。

【问题 4】(4 分)

该校园网在安全设计上采用分层控制方案，将整个网络分为外部网络传输控制层、内外网间访问控制层、内部网络访问控制层、操作系统及应用软件层和数据存储层，对各层的安全采取不同的技术措施。从备选答案中选择信息，将表 14.3 中的(11)～(14)处空缺信息填写在对应的位置。

表 14.3　安全技术和对应层次

安全技术	对应层次
__(11)__	外部网络传输控制层
__(12)__	内外网间访问控制层
__(13)__	内部网络访问控制层
__(14)__	数据存储层

(11)～(14)题备选答案：

A. IP 地址绑定　　B. 数据库安全扫描

C. 虚拟专用网(VPN)技术　　D. 防火墙

试题二(15 分)

阅读以下说明，回答问题 1 至问题 3。

【说明】

如图 14.18 所示，某单位通过 2Mb/s 的 DDN 专线接入广域网，该单位内网共分为 3 个子网。服务器放置在子网 192.168.5.1/24 中，财务部工作站放置在子网 192.168.10.1/24，销售部工作站放置在子网 192.168.50.1/24。该单位申请的公网 IP 地址为 61.246.100.97/29。

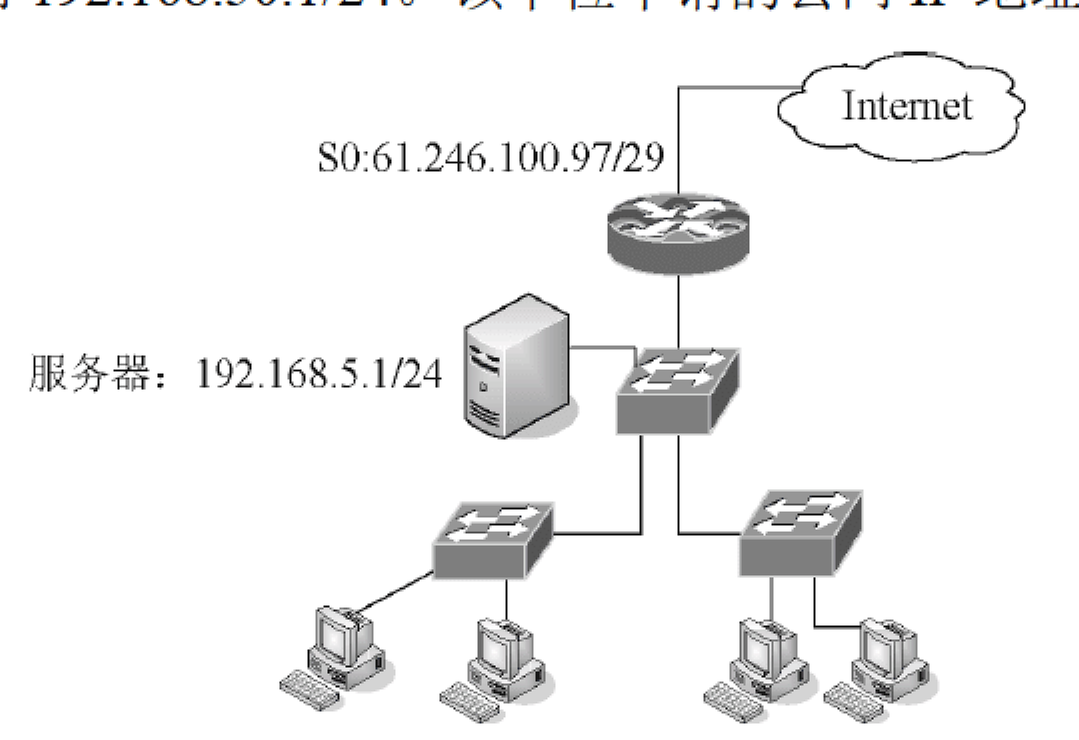


图 14.18　某单位网络连接

【问题 1】(3 分)

该单位的公网 IP 地址范围是 (1) 到 (2) ；其中该单位能够使用的有效公网地址有 (3) 个。

【问题 2】(6 分)

为保证路由器的安全，网络管理员做了如下设置，请阅读下列 3 段路由配置信息，并在(4)～(6)处填写该段语句的作用。

```
1. Router(Config)#no ip http server                              (4)
2. Router(Config)#snmp-server community admin RW                 (5)
3. Router(Config)#access-list 1 permit 192.168.5.1
   Router(Config)#line con 0
   Router(Config-line)#transport input none
   Router(Config-line)#login local
   Router(Config-line)#exec-timeout 5 0
   Router(Config-line)#access-class 1 in                         (6)
```

【问题 3】(6 分)

请参照图 14.18，在路由器上完成销售部网段 NAT 的部分配置。

```
…
Router(config)#ip nat pool xiaoshou 61.246.100.99 61.246.100.99 netmask  (7)
//设置地址池
//
Router(config)#access-list 2 permit  (8)   (9)
//定义访问控制列表
//
Router(config)#ip nat inside source list 2 pool xiaoshou
//使用访问控制列表完成地址映射
```

试题三(15 分)

阅读以下关于 Linux 网关安装和配置过程的说明，回答问题 1 至问题 5。

【说明】

当局域网中存在大量计算机时，根据业务的不同，可以将网络分成几个相对独立的子网。图 14.19 是某公司子网划分的示意图，整个网络被均分为销售部和技术部两个子网，子网之间通过一台安装了 Linux 操作系统的双网卡计算机联通。

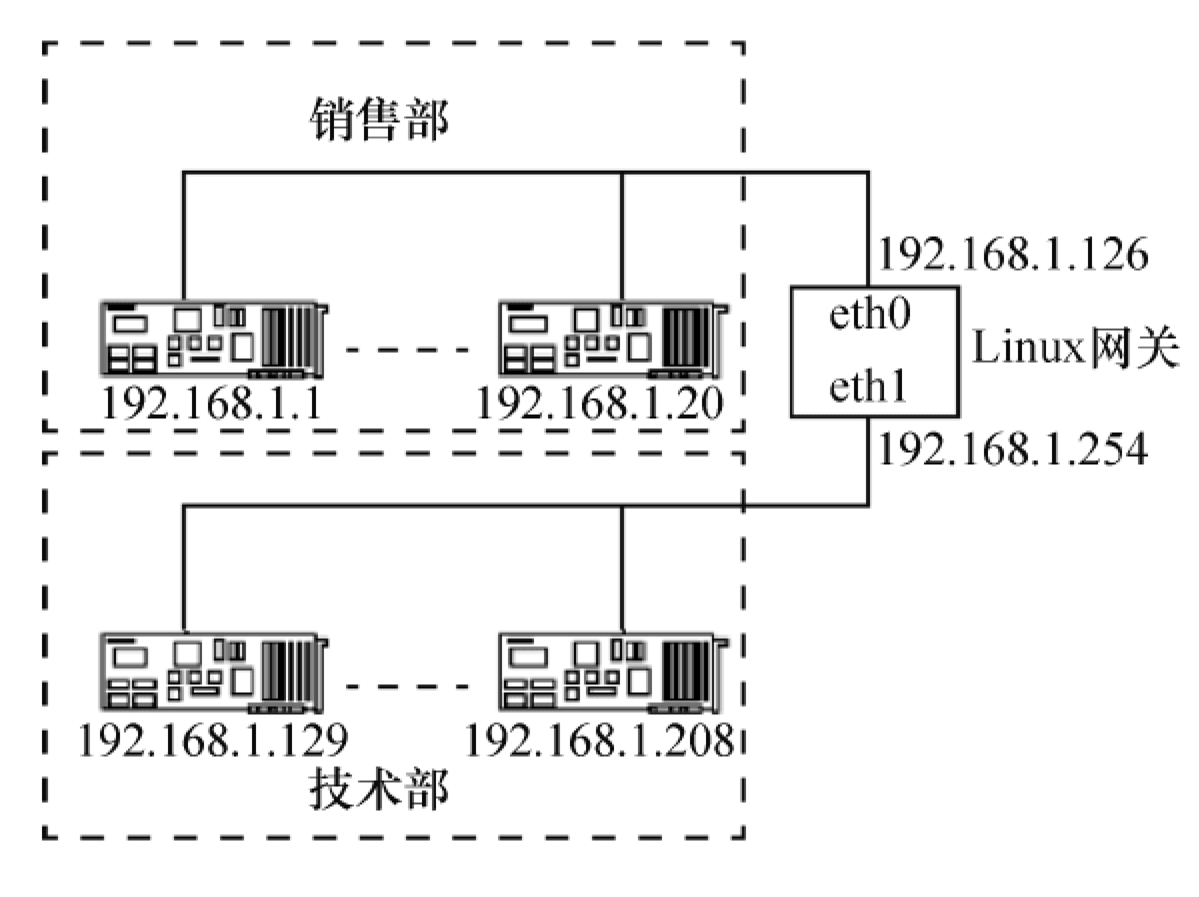


图 14.19 子网划分示意图



【问题 1】(5 分)

销售部的网络号是_(1)_，广播地址是_(2)_；技术部的网络号是_(3)_，广播地址是_(4)_；每个子网可用的 IP 地址有_(5)_个。

【问题 2】(3 分)

Linux 网关计算机有两个网络接口(eth0 和 eth1)，每个接口与对应的子网相连接。

该计算机/etc/sysconfig/network 文件清单为：

```
NETWORKING=yes
FORWARD_IPV4=__(6)__
HOSTNAME=gateway.ABC.com
```

/etc/sysconfig/network-scripts/ifcfg-eth0 文件清单为：

```
DEVICE=eth0
IPADDR=192.168.1.126
NETMASK=__(7)__
```

…

/etc/sysconfig/network-scripts/ifcfg-eth1 文件清单为：

```
DEVICE=eth1
IPADDR=192.168.1.254
NETMASK=__(8)__
```

…

(6)题备选答案：A. yes　　B. no　　C. route　　D. gateway

【问题 3】(2 分)

在网关计算机/etc/sysconfig/network-scripts/目录中有以下文件，运行某命令可以启动网络，该命令是_(9)_，其命令行参数是_(10)_。

```
ifcfg-eth0          ifup              ifup-sit
ifcfg-lo            ifup-aliases      ifup-sl
ifdown              ifup-cipcb        ifup-wireless
ifdown-aliases      ifup-ippp         init. ipv6-global
ifdown-cipcb        ifup-ipv6         network-functions
ifdown-ippp         ifup-ipx          network-functions-ipv6
ifdown-ipv6         ifup-isdn
ifdown-isdn         ifup-plip
ifdown-post         ifup-plusb
ifdown-ppp          ifup-post
ifdown-sit          ifup-ppp
ifdown-sl           ifup-routes
```

【问题 4】(2 分)

在网关计算机上使用以下路由命令创建两个默认的路由。

route add-net 192.168.1.0　　255.255.255.128　　_(11)_

route add-net 192.168.1.128　　255.255.255.128　　_(12)_

【问题 5】(3 分)

设置技术部和销售部的主机网络参数后，如果两个子网间的主机不能通信，用_(13)_命

令来测试数据包是否能够到达网关计算机。如果数据包可以达到网关但是不能转发到目标计算机上，则需要用命令 cat/proc/sys/net/ipv4/ip_forward 来确认网关计算机的内核是否支持 IP 转发。如果不支持，则该命令输出 (14) 。

(13) A. traceroute　　B. tracert　　C. nslookup　　D. route

(14) A. 1　　B. 0　　C. yes　　D. no

试题四(15 分)

阅读以下说明，回答问题 1 至问题 6。

【说明】

某公司在 Windows Server 2003 中安装 IIS 6.0 来配置 Web 服务器，域名为 www.abc.com。

【问题 1】(2 分)

IIS 安装的硬盘分区最好选用 NTFS 格式，是因为 (1) 和 (2) 。

A. 可以针对某个文件或文件夹中不同的用户分配不同的权限

B. 可以防止网页中的 Applet 程序访问硬盘中的文件

C. 可以使用系统自带的文件加密系统对文件或文件夹进行加密

D. 可以在硬盘分区中建立虚拟目录

【问题 2】(3 分)

为了禁止 IP 地址为 202.161.158.239～202.161.158.254 的主机访问该网站，在图 14.20 所示的“IP 地址和域名限制”对话框中单击“添加”按钮，增加两条记录，如表 14.4 所示。填写表 14.4 中(3)～(5)处内容。



图 14.20　IP 地址和域名限制

表 14.4　增加的两条记录

	IP 地 址	子网掩码
一组主机	(3)	(4)
一台主机	(5)	

【问题 3】(4 分)

实现保密通信的 SSL 协议工作在 HTTP 层和 (6) 层之间。SSL 加密通道的建立过程如下。

1. 首先客户端与服务器建立连接，服务器把它的 (7) 发送给客户端。

2. 客户端随机生成 (8) ，并用从服务器得到的公钥对它进行加密，通过网络传送给服务器。

3. 服务器使用 (9) 解密得到会话密钥，这样客户端和服务器端就建立了安全通道。

(6)～(9)备选答案：

A. TCP　　B. IP　　C. UDP　　D. 公钥　　E. 私钥

F. 对称密钥　　G. 会话密钥　　H. 数字证书　　I. 证书服务

【问题 4】(2 分)

在 IIS 中安装 SSL 分 5 个步骤，这 5 个步骤的正确排序是__(10)__。

A. 配置身份验证方式和 SSL 安全通道　　B. 证书颁发机构颁发证书

C. 在 IIS 服务器上导入并安装证书　　D. 从证书颁发机构导出证书文件

E. 生成证书请求文件

【问题 5】(2 分)

在安装 SSL 时，在“身份验证方法”对话框中应选用的登录验证方式是__(11)__。

A. 匿名身份验证　　B. 基本身份验证

C. 集成 Windows 身份验证　　D. 摘要式身份验证

E. Net Passport 身份验证

【问题 6】(2 分)

如果用户需要通过 SSL 安全通道访问该网站，应该在 IE 地址栏中输入__(12)__。SSL 默认侦听的端口是__(13)__。

试题五(15 分)

阅读下面的说明，回答问题 1 至问题 4。

【说明】

图 14.21 是某公司利用 Internet 建立的 VPN。

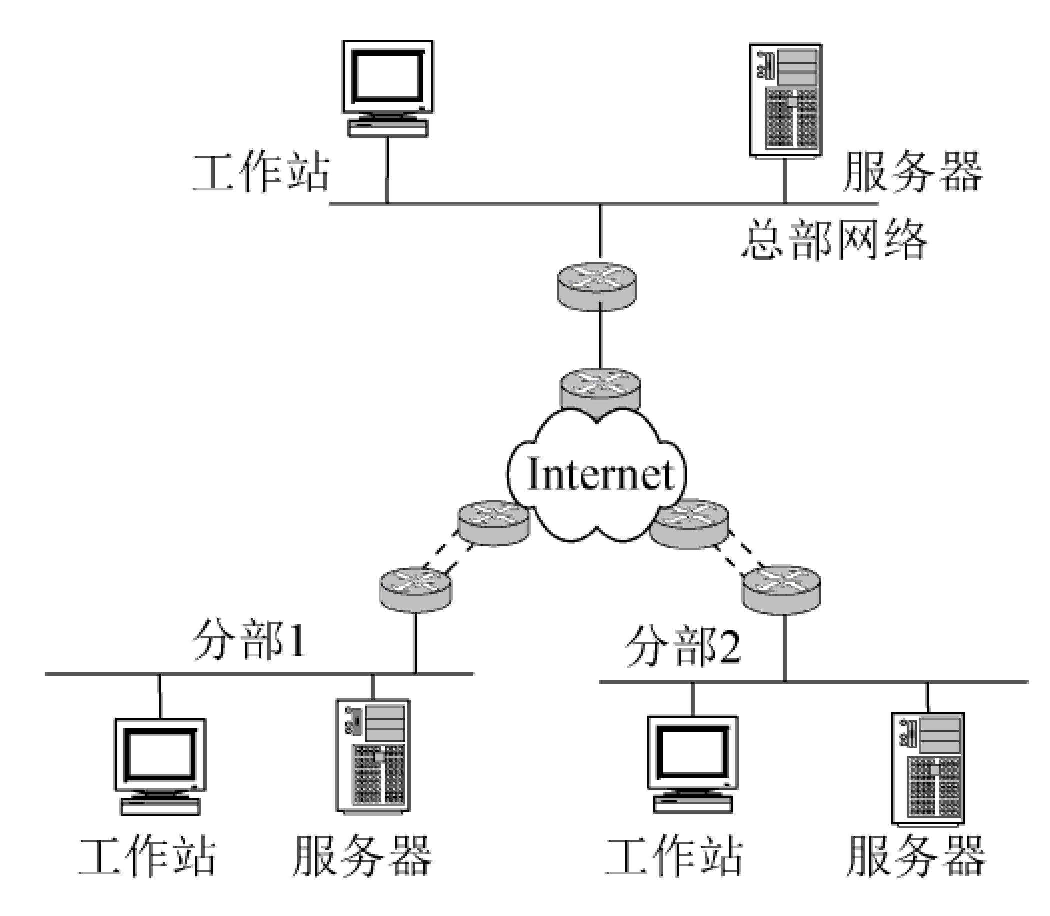


图 14.21　某公司 VPN

【问题 1】(4 分)

使用 VPN 技术，是为了保证内部数据通过 Internet 安全传输，VPN 技术主要采用哪些技术来保证数据安全？

【问题 2】(3 分)

分部 1 采用 DDN 通过一台路由器接入 Internet。 阅读下面的路由配置信息，将(1)～(3)处标识的语句进行解释。

```
Router>en                                        (进入特权模式)
Router#config terminal                           (进入全局配置模式)
Router(config)#enable secret cisco               (设置特权口令)
Router(config)#line vty 0 4
Router(config-line)#password goodbad             ____(1)____
Router(config-line)#exit
Router(config)#interface eth0/0                  (进入以太网接口配置模式)
Router(config-if)#ip address 202.117.1.1 255.255.255.0
                                                 (设置 IP 地址和掩码)
Router(config-if)#no shutdown                    (启用以太网接口)
Router(config-if)#exit
Router(config)#interface serial0/0               (进入串口配置模式)
Router(config-if)#ip address 211.175.132.10 255.255.255.252
                                                 (设置 IP 地址和掩码)
Router(config-if)#bandwidth 256                  (指定带宽为 256KB)
Router(config-if)#encapsulation  ppp             ____(2)____
Router(config-if)#no cdp enable                  ____(3)____
Router(config-if)#no shutdown                    (启用 serial 接口)
Router(config-if)#exit
Router(config)#
```

【问题 3】(4 分)

分部 1 的路由器配置为 ethernet0/0 端口接内部网络，serial0/0 端口接外部网络。下列配置指定内外网端口，完成下列配置，将答案填写在答题纸相应的位置。

```
Router(config)#inter eth0/0
Router(config-if)#____(4)____
Router(config-if)#inter serial0/0
Router(config-if)#____(5)____
Router(config-if)#exit
Router(config)#
```

【问题 4】(4 分)

以下是指定 VPN 在建立连接时协商 IKE 使用的策略，阅读下面的配置信息，解释(6)、(7)处的命令，将答案填写在答题纸相应的位置。

```
Router(config)#crypto isakmp policy 10           (定义策略为 10)
Router(config-isakmp)#hash md5                   ____(6)____
Router(config-isakmp)#authentication pre-share   ____(7)____
Router(config-isakmp)#exit
Router(config)#crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
                        (配置预共享密钥为 cisco123，对等端为所有 IP)
```

14.2 参考答案与解析

14.2.1 考前模拟卷 1 参考答案与解析

上午科目答案与解析

(1) 答　案：C。

解　析：内存地址区间为 4000H～43FFH，则该内存的存储单元个数为

43FFH−4000H+1=400H=1024。若每个存储单元可存储 16 位二进制数，则该内存的存储容量为 1024×16/8=2048B。该内存区域由 4 片存储器芯片构成，则所需要的芯片的容量为 2048/4=512 B。选项 A 中的芯片容量为 1024 B，选项 B 中的芯片容量为 256 B，选项 D 中的芯片容量为 1024 B。

(2) 答　案：D。

解　析：平均故障时间与失效率的关系为 MTBF=1/λ，则计算机系统的总失效率为系统平均故障间隔时间的倒数，即 10^{-5}/小时。对于串联系统，计算机系统的总失效率为各部件失效率的和，因此，另一个部件的效率应为 10^{-5}/小时−7×10^{-6}/小时=3×10^{-6}/小时。

(3) 答　案：B。

解　析：计算机的主存通常使用性价比高的 DRAM 芯片，该芯片的工作速度与 CPU 的工作速度不匹配，例如 733 MHz 的奔腾 III CPU，一次指令的执行时间为 1.35 ns，与其相配的主存存取时间为 7 ns，后者是前者的 5 倍。在 CPU 与主存之间设置高速缓冲存储器 Cache 是减小内存与 CPU 之间速度差异的途径之一。

高速缓冲存储器(Cache)所用芯片都是高速的，其存取速度可与微处理器相匹配，容量由几十 KB～几百 KB，通常用来存储当前使用最多的程序或数据。Cache 位于 CPU 与主存储器之间，每次访问存储器时，都先访问高速缓存，若访问的内容在高速缓存中，访问到此为止；否则，再访问主存储器，并把有关内容及相关数据块取入高速缓存。这样，如果大部分针对高速缓存的访问都能成功，则在主存储器容量保持不变的情况下，访问速度可接近高速缓存的存取速度，这无疑可提高微机的运行速度。

(4) 答　案：B。

解　析：衡量模块独立度的标准是耦合性和内聚性。耦合性是指软件系统结构中各模块间相互连系的紧密程度的一种度量，模块之间的联系聚合越紧密，其耦合性就越强，模块的独立性就越差。内聚性是一个模块内各个元素彼此结合的紧密程度的度量，一个模块内各个元素的联系越紧密，其内聚性就越高，模块的独立性就越好。因此提高内聚性，降低模块之间的耦合性是模块设计应该遵循的最重要的两个原则。

(5) 答　案：D。

解　析：多级目录结构像一棵倒置的有根树，所以也称为树型目录结构。从树根向下，每一个节点都是一个目录，叶节点是文件。采用多级目录结构的文件系统中，用户要访问一个文件，必须指出文件所在的路径名。路径名包含从根目录开始到该文件的通路上所有各级目录名。因此，对于具有相同文件名的文件，当用户使用不同的目录，便不会重名。这就是文件系统容许不同用户的文件可以具有相同的文件名的原因。

(6) 答　案：A。

解　析：数据流图是结构化分析方法中用于表示系统逻辑模型的一种工具，它以图形的方式描绘数据在系统中流动和处理的过程。而结构化分析是一种面向数据流的需求分析方法，可见数据流图是需求分析阶段产生的结果。

(7) 答　案：C。

解　析：进程由就绪状态到运行状态是由调度程序的调度引起；而进程由运行状态到就绪状态是由于时间片用完引起；进程由运行到阻塞状态的转换是由于等待某事件(如 I/O 请求)引起的；进程由阻塞到就绪状态的转换是由于 I/O 完成或等待的事件发生引起的。

(8) 答　案：D。

解　析：在面向对象的软件工程中，类可以用预先开发的源代码来实现，这些源代码就称为组件(Component)，从而简化了面向对象环境的产生，故答案选 D。

(9) 答　案：C。

解　析：Gantt 图能清晰地描述每个任务从何时开始，到何时结束以及各个任务之间的并行性，但是它不能清晰地反映出各任务之间的依赖关系，难以确定整个项目的关键所在，也不能反映计划中有潜力的部分，故答案选 C。

(10) 答　案：B。

解　析：根据我国《专利法》第九条的规定：“两个以上的申请人分别就同样的发明创造申请专利的，专利权授予最先申请的人。”

(11) 答　案：B。

解　析：根据 Nyquist 定理可知，理想信道的码元速率为 B=2W(Baud)，其中 W 为信道带宽。

数据速率还取决于码元的离散状态数，码元携带的信息量 n(比特数)与码元的离散状态数 N 的关系为 $n=\log_2 N$。可得信道的数据速率为 $R=B\log_2 N=2W\log_2 N=2\times4000\times\log_2 4=16\ 000$ b/s=16 Kb/s。

(12) 答　案：A。

解　析：单模光纤纤芯直径很小，理论上只能传导一种模式的光，从而避免了模间色散，光在其中无反射地沿直线传播，因此具有较高的数据速率，传输距离较长，但成本较高。多模光纤可传多种模式的光，模间色散较大，因此传输速率较低，传输距离较短。

(13) 答　案：D。

解　析：曼彻斯特编码是一种双相码，通常用高电平到低电平的转换边表示 0，用低电平到高电平的转换边表示 1。双相码的特点是每一位中都有一个电平转换，因而这种代码的最大优点是自定时。曼彻斯特编码每一个码元都要调制为两个不同的电平，因而调制速率是码元速率的两倍，也就是说编码效率只有 50%，可见曼彻斯特编码效率不高。

(14) 答　案：B。

解　析：DPSK 是一种差分相位调制技术，即用不同的相位变化表示数据，例如对于位 0，前沿有相位变化，对于位 1，前沿没有相位变化。

(15)和(16)答　案：(15)B；(16)B。

解　析：E1 载波把 32 个 8 位一组的数据样本组装成 125μs 的基本帧，其中 30 个子信道用于话音传送数据，2 个子信道用于传送控制信令。可计算出 E1 载波的数据速率为 256 b/125 μs=2.048 Mb/s，每个话音信道的数据速率为 8 b/125 μs=64 Kb/s。

(17) 答　案：B。

解　析：8 个 9600 b/s 的信道复用在一条线路上，按照同步时分多路方式计算，复用线路的带宽为 9600 b/s×8=76.8 Kb/s。在统计 TDM 情况下，每个子信道有 80%的时间忙，复用线路的控制开销为 5%，则复用线路的带宽为 76.8 Kb/s×80%×105%≈64 Kb/s。

(18) 答　案：D。

解　析：由监督关系式可知，c_0 校验 x_1、x_3、x_5、x_7 这 4 位，结果为 1；c_1 校验 x_2、x_3、x_6、x_7 这 4 位，结果为 0；c_2 校验 x_4、x_5、x_6、x_7 这 4 位，结果为 1。$c_2c_1c_0=(101)_2=5$，由此



可见第 5 位发生了错误，需要将第 5 位的 0 变为 1，因此答案选 D。

(19) 答　案：D。

解　析：ADSL 宽带接入使用的是 PPPoE 协议。PPPoE 提供了一种理想的接入方案，即通过一个简单的共享接入设备将多个客户网段接入到宽带骨干网络。 在实际的应用中，PPPoE 利用以太网的工作机理，将 ADSL Modem 的 10Base-T 接口与内部以太网互连，实现 PPP 的动态接入。

PPP 协议是一种有效的点对点通信协议，用于通过串行接口连接的两台计算机之间的通信。如果用户使用 Windows 中的拨号连接，则需要使用调制解调器，通过 PPP 协议建立会话。

SLIP 协议可使远程用户通过电话线及高速调制解调器方便地接入 TCP/IP 网络。

(20) 答　案：C。

解　析：选项 A 的 LAP-B 是 X.25 的数据链路层协议，帧中继使用 LAP-D；选项 B 的 X.21 用于定义主机与物理网络之间物理、电气、功能以及过程特性，是 X.25 的物理层协议；选项 D 的 MHS 是信息处理服务，是 OSI/RM 应用层协议。X.25 PLP 是 X.25 的网络层协议，故答案为 C。

(21) 答　案：D。

解　析：路由器是网络层设备，利用互联网协议将网络分成几个逻辑子网。路由器基于第三层 IP 地址来决定是否进行分组转发，如果分组的源地址和目的地址在同一网络中，则分组不会被路由器转发；如果源地址和目的地址不在同一网络中，那么路由器会转发该分组。这就起到隔离子网的作用。同时路由器还可以抑制广播风暴，当路由器收到目的地址为 255.255.255.255 的广播分组时不会转发，从而广播被局限于一个网络中，不会渗透到其他网络中。

网络地址转换(NAT)技术是在路由器上实现的。NAT 技术用于把私网地址转换成公网地址，或者进行相反的转换。

一个路由器往往会从多个途径得到某指定网络的路由信息。当有多条最佳路径时，路由器会选择一个路由信息源可信度最高的路径。

IP 分组的传播方式有单播、组播和广播。如果分组的 IP 地址中主机号全是 1，那么该地址是直接广播地址，路由器会将该分组以广播方式发送给特定网络上的所有主机。D 类地址为组播地址，如果路由器判断目标地址为组播地址，则会将分组转发到需要的主机和网络。可见，路由器可以实现点到多点的传输。所以选项 D 是错误的。

(22) 答　案：C。

解　析：选项 A 所描述的是 ARP 协议的功能，选项 B 所描述的是 NAT 协议的功能，选项 D 所描述的是 DHCP 协议的功能，答案选 C。

(23) 答　案：B。

解　析：TCP 报文段头部的前 20 个字节是固定的，包括 16 位源端口、16 位目标端口、32 位发送顺序号、32 位接收顺序号、4 位偏置值、6 位保留字段、6 位标志字段、16 位窗口、16 位检查和 16 位紧急指针；段头的后面 $4n$ 字节是可选项。可知 TCP 段头的最小长度是 20 字节。

(24) 答　案：B。

解　析：UDP 协议提供了不可靠的无连接的传输服务，每个数据包都是相互独立的，不需要顺序号来标记。而选项 A、C、D 中的内容在 TCP 头和 UDP 头中都有，故答案选 B。

(25)和(26) 答　案：(25)A；(26)A。

解　析：在 Internet 中用地址解析协议 ARP 来实现 IP 地址到 MAC 地址的映像。ARP 协议利用了以太网的广播特性，将 ARP 报文封装在以太网的数据帧中传送。

(27) 答　案：D。

解　析：OSPF 是一种分层的路由协议，自治系统被划分为多个区域，每个区域是运行路由选择算法的一个实例，连接多个区域的路由器运行路由选择算法的多个实例。

路由器启动时，首先初始化路由协议的数据结构并等待下层协议的指示，得到下层的工作指示后就利用 Hello 协议来发现邻居路由器。在广播网络和点对多点网络中，路由器向各个活动端口组播 Hello 分组，并接收邻居发来的 Hello 分组。

在广播网络中，Hello 协议还用来选择指定路由器。Hello 分组中包含了发送路由器的优先级，优先级最高的路由器成为指定路由器。

OSPF 是一种链路状态协议，链路状态协议与距离矢量协议发布路由信息的方式不同，链路状态协议是在网络拓扑发生变化时才发布路由信息，而距离矢量协议是周期性地发布路由信息，所以链路状态协议没有固定的路由更新周期，而距离矢量协议具有设定的路由更新周期，例如 RIP 协议的路由更新周期为 30s。

(28) 答　案：A。

解　析：链路状态协议与距离矢量协议发布路由信息的方式不同，主要有以下 4 点区别。

- 链路状态协议是在网络拓扑发生变化时才发布路由信息，而距离矢量协议是周期性地发布路由信息。
- 链路状态协议是由广播网络内部指定的路由器发布路由信息，而距离矢量协议的所有路由器都发布路由信息。
- 链路状态协议采用组播方式发布路由信息，而距离矢量协议则是广播路由信息。
- 链路状态协议发布的组播报文要求应答，这种通信方式比不要求应答的广播通信更可靠。

因此答案选 A。

(29) 答　案：C。

解　析：FTP(文件传输协议)主要用于 Internet 上文件的双向传输。FTP 服务采用客户机/服务器模式。客户机和服务器之间利用 TCP 建立连接，保证文件传输的可靠性。

TFTP(简单文件传送协议)的功能与 FTP 类似，但是为了保持简单和短小，TFTP 使用 UDP 协议。

(30) 答　案：C。

解　析：title 是元素标记名称；style 是元素标记属性名称；italic 是元素标记属性值；science 是元素内容。

(31) 答　案：B。

解　析：FTP 采用了客户端/服务器模型。客户端和服务器之间要建立两条 TCP 连接，一条用于传送控制信息，另一条用于传送文件内容。控制连接的建立使用的是被动模式，即服务器进程以被动方式在 TCP 的 21 号端口上打开，等待客户端的连接；当用户访问 FTP



服务器时，客户端的进程以主动的方式在一个 TCP 随机端口上打开，请求与服务器建立连接。

(32) 答　案：D。

解　析：交换机有多种，共同的特点都是根据某种标识把输入数据包交换到输出端口。以太网交换机根据 MAC 地址进行交换；帧中继交换机根据虚电路号 DLCI 进行交换；Internet 中使用的三层交换机根据 IP 地址进行转发，并根据 MAC 地址进行交换；ATM 交换机根据虚电路标识 VPI 和 VCI 进行交换。

(33)和(34) 答　案：(33)B；(34)B。

解　析：由以上信息的第 4 和第 5 行

```
Administrative mode: trunk
Operational Mode: trunk
```

可知交换机端口处于中继连接状态；

由第 8 行

```
Negotiation of Trunking: Disabled
```

可知不要求与对方建立中继连接。

由第 10 行

```
Trunking Native Mode VLAN: 1(default)
```

可知默认的 VLAN 为 VLAN1。

(35) 答　案：A。

解　析：show 命令可以帮助获得监控路由器的重要信息。在用户模式下，可以查看路由器系统的一般信息，如系统时钟、系统的软硬件版本等；在特权模式下，可以查看路由器的配置、IP 的相关信息、路由表信息等。因此，要显示路由器的运行配置需要在特权模式下操作，可以排除选项 C、D。R1 # show running-config 命令是显示运行文件，R1 # show startup-config 命令是重新显示启动文件，因此正确答案为 A。

(36) 答　案：B。

解　析：在 Samba 服务器配置文件 smb.conf 中，workgroup 项表示在 Windows 操作系统中的“网上邻居”中将会出现的 Samba 服务器所属群组，默认为 MYGROUP，不区分大小写。server string 项是 Samba 服务器的注释说明。netbios name 项定义 netbios 名字，该名字在“网上邻居”中出现。guest account 项设定访问 samba server 的来宾账户(即访问时不用输入用户名和密码的账户)，若设为 pcguest 的话，则默认为 nobody 用户。

(37) 答　案：C。

解　析：在 Linux 系统中，cat 命令用来在屏幕上滚动显示文件内容；more 命令可以分页显示文件内容；cp 为文件复制命令。

(38) 答　案：B。

解　析：本题描述中所提到的 IP 地址 169.254.220.167 实际上是自动私有 IP 地址。当 DHCP 客户端无法与 DHCP 服务器通信时，在 Windows 2000 以前的系统中，如果计算机无法获取 IP 地址，则自动配置成“IP 地址：0.0.0.0”“子网掩码：0.0.0.0”的形式，导致其不能与其他计算机进行通信。而对于 Windows 2000 以后的操作系统，则在无法获取 IP 地

址时自动设置成“IP 地址：169.254. ×. ×”“子网掩码：255.255.0.0”的形式，这样可以使所有获取不到 IP 地址的计算机之间能够通信。

(39)和(40) 答　案：(39)C；(40)A。

解　析：在 Apache 服务器的配置文件 httpd.conf 中，NameVirtualHost 用来指定虚拟主机使用的 IP 地址，这个 IP 地址将对应多个 DNS 名字。如果 Apache 使用 Listen 参数控制了多个端口，那么就可以在这里加上端口号以进一步进行区分对不同端口的不同连接请求。此后，使用 VirtualHost 语句，使用 NameVirtualHost 指定的 IP 地址作参数，对每个名字都定义对应的虚拟主机设置。

按照题目要求，用户可通过 http://www.test.cn 访问到该 Apache 服务器，而配置文件中 ServerName 缺少，所以(40)处应填入 www.test.cn，当用户访问 http://111.25.4.30:80 时，会访问配置文件中定义的第一个虚拟主机 www.othertest.com。

(41) 答　案：C。

解　析：代理服务器是介于浏览器和 Web 服务器之间的一台服务器，当用户通过代理服务器上网浏览时，浏览器不是直接到 Web 服务器上去取回网页，而是向代理服务器发出请求，由代理服务器来取回浏览器所需要的信息并传送到用户的浏览器。使用代理服务器访问 Internet 时可以突破对某些网站的访问权限，提高访问某些网站的速度，隐藏本地主机的 IP 地址，但是不能避免来自 Internet 上的病毒入侵。

(42) 答　案：C。

解　析：Windows Server 2003 采用了活动目录技术，域间信任关系有多种形式，还采用了多主机复制模式，多个域控制器没有主次之分，域中每个域控制器既可接受其他域控制器的变化信息而改变目录信息，也可把变化的信息复制到其他域控制器。

(43) 答　案：D。

解　析：Windows Server 2003 在系统安装完毕后，会自动建立几个特殊组，其中包括 Interactive(任何在本机登录的用户)、Network(任何通过网络连接的用户)、Everyone(任何使用计算机的人员)和 System(系统组)等。而终端服务可以让操作者通过远程访问服务器桌面。默认情况下，只有系统管理员组和系统组用户拥有访问和完全控制终端服务器的权限。

(44) 答　案：A。

解　析：DES(Data Encryption Standard)是 20 世纪 70 年代制定的密码算法。DES 的加密密钥和解密密钥相同，属于对称密码体制。

(45)和(46) 答　案：(45)A；(46)D。

解　析：数字证书是各类终端实体和最终用户在网上进行信息交流及商务活动的身份证明，而这一前提是保证数字证书本身的有效性。验证数字证书的有效性是通过验证颁发证书的 CA 的签名实现的。

(47) 答　案：C。

解　析：隧道技术、加解密技术、密钥管理技术和身份认证技术是实现 IPSec VPN 的关键技术。隧道技术是一种通过使用因特网基础设施在网络之间传递数据的方式；加解密技术可实现保密通信，保证公司业务和个人通信的安全；加入 VPN 的用户都要通过身份认证，通常使用用户名和密码，或者智能卡来实现用户的身份认证。

(48) 答　案：D。





解　析：PGP(Pretty Good Privacy)是一个基于 RSA 公钥加密体系的邮件加密软件。可以用它对邮件保密以防止非授权者阅读，还能对邮件加上数字签名，从而使收信人可以确信邮件是原发送方所发来的。它让用户可以安全地和从未见过的另一方通信，事先并不需要任何保密的渠道用来传递密钥。PGP 也可以用来加密文件，因此 PGP 已经成为使用最广泛的电子邮件加密软件。但 PGP 不能压缩电子邮件的大小。

(49) 答　案：B。

解　析：在桌面上右击“我的电脑”图标，从弹出的快捷菜单中选择“管理”命令，调出“计算机管理”窗口，事件查看器允许用户监视应用程序、安全性和系统日志中记录的事件，如图 14.22 所示。答案为 B。



图 14.22　“计算机管理”窗口

(50)和(51) 答　案：(50)C；(51)C。

解　析：ipconfig 是最常用的 Windows 使用程序，可以显示所有网卡的 TCP/IP 配置参数，可以刷新动态主机配置协议和域名系统的设置。ipconfig /all 显示所有网卡的 TCP/IP 配置信息。

ping 命令通过向目标主机发送一个 ICMP 回送请求数据包来检验与另一个计算机的连接。

netstat 命令的功能是显示 TCP 连接、计算机正在监听的端口、以太网统计信息、IP 路由表、IPv4 统计信息和 IPv6 统计信息等。

nslookup 命令用于显示 DNS 查询信息。

(52) 答　案：B。

解　析：有两种威胁是安全体系结构不必防护的，因为它们不是很重要，或者这种防护没有多大作用。

拒绝服务：因为在很多情况下拒绝服务和网络失效是无法区别的，所以可以由网络管理协议来处理，安全子系统不必采取措施。

通信分析：即由第三者分析管理实体之间的通信规律，从而获取需要的信息。由于通常都是由少数管理站来管理整个网络的，所以管理系统的通信模式是可预见的，防护通信分析就没有多大作用了。

(53) 答　案：D。

解　析：netstat 命令的用法如下：

```
netstat [-a] [-e] [-n] [-s] [-p proto] [-r] [interval]
```

其中：

-a 显示所有连接和处于监听状态的接口(服务器端的连接通常不显示)。

-e 显示以太网统计信息。

-s 显示每个协议的统计数据，默认显示 TCP、UDP 和 IP 的统计数据；利用-p 选项可以指定只显示其中一部分。

-r 显示路由表的内容。

(54) 答　案：B。

解　析：RAID1 磁盘利用率只有 50%，是所有 RAID 上磁盘利用率最低的一个级别。RAID0 的磁盘利用率最高，可达 100%，RAID3、RAID5 硬盘利用率为$(n-1)/n$。

(55) 答　案：C。

解　析：标准规定的私网地址如下。

1 个 A 类网络，包含的地址有：10.0.0.0～10.255.255.255。

16 个 B 类网络，包含的地址有：172.16.0.0～172.31.255.255。

256 个 C 类网络，包含的地址有：192.168.0.0～192.168.255.255。

(56)和(57) 答　案：(56)C；(57)C。

解　析：把网络 202.100.192.0/18 划分成 30 个子网，需要从 14 位主机号中借用高 5 位来标识子网号，还留有 9 位来标识主机地址，则子网掩码为 11111111 11111111 11111110 00000000，即 255.255.254.0。每个子网可分配的主机地址数为 $2^9-2=510$(个)。

(58) 答　案：D。

解　析：校园网地址块 202.105.192.0/18 的网络号是 18 位，C 类网络的主机号是 8 位，则子网号是 6 位，所以该校园网包含了 62 个 C 类网络。

(59) 答　案：C。

解　析：在交换机上实现 VLAN，可以采用静态的或动态的方法。

静态方法是基于端口来划分 VLAN，为交换机的各个端口指定所属的 VLAN。

动态分配可以根据设备的 MAC 地址、网络层协议、网络层地址、IP 广播或管理策略来划分 VLAN。基于 MAC 地址划分 VLAN 是按每个连接到交换机设备的 MAC 地址定义 VLAN 成员；根据上层协议、逻辑地址来划分 VLAN，有利于组成基于应用的 VLAN。

(60) 答　案：A。

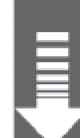
解　析：按端口划分属于静态划分方法，各个端口固定地分配给不同的 VLAN。而按 MAC 地址、协议类型或逻辑地址划分都属于动态划分方法。

(61) 答　案：A。

解　析：ip route 命令的格式为<ip route+目的网络地址+子网掩码+下一跳路由器 IP 地址>。因为路由器 R1 与路由器 R2 相连，且路由器 R2 直接与 Internet 上的路由器相连，所以路由器 R1 的下一跳路由器为路由器 R2。所以正确的配置应为 ip route 0.0.0.0 0 0.0.0.0 212.112.8.6。

(62) 答　案：B。

解　析：IEEE 802 标准把数据链路层划分成了两个子层，与物理介质相关的部分叫作介质访问控制(MAC)子层，与物理介质无关的部分叫作逻辑链路控制(LLC)子层。对应的 IEEE 802 局域网中的地址也分为两级，即主机的地址是 MAC 地址；LLC 地址是 LLC 层服



务访问点，实际上是主机中上层协议实体的地址。一个主机可以同时拥有多个上层协议进程，因而就有多个服务访问点。

(63) 答　案：B。

解　析：CSMA/CD 是一种解决访问冲突的协议，可以有效地实现多节点对共享传输介质的访问控制，在 CSMA/CD 方法的基础上形成了 IEEE 802.3 标准。

CSMA/CD 方法用来保证每个节点都能“公平”使用公共传输介质，但随着局域网规模的不断扩大，节点数不断增加，每个节点平均分配的带宽越来越少，冲突和重发现象将大量发生，网络效率将会急剧下降，网络传输延迟将会增长，网络服务质量将会下降。可见，在网络负载较小时，CSMA/CD 协议的通信效率很高，而网络负载变大时，则通信效率会降低。

快速以太网的协议标准是 IEEE 802.3u，该标准在 MAC 子层使用 CSMA/CD 方法，提供 10 Mb/s 与 100 Mb/s 的自动协商功能。快速以太网支持全双工与半双工两种工作模式，这是它与传统以太网一个很大的区别。传统的以太网只能以半双工方式工作，不能同时收发数据，主机之间需要争用共享的传输介质，因此就出现了 CSMA/CD 方法。而在全双工模式下工作，主机有两个通道，一个用于接收数据，一个用于发送数据。支持全双工模式的快速以太网的拓扑结构一定是星型，这种连接方式不存在争用问题，因此不需要采用 CSMA/CD 方法。千兆以太网也有两种工作模式，在全双工工作模式下不需要采用 CSMA/CD 协议。万兆以太网只有全双工工作模式，不需要采用 CSMA/CD 协议。

(64) 答　案：D。

解　析：万兆以太网标准由 IEEE 802.3ae 委员会指定，正式标准在 2002 年 6 月发布，该标准支持 10 Gb/s 的传输速率。IEEE 802.3u 是快速以太网的标准，IEEE 802.3z 是千兆以太网的标准。

(65)和(66) 答　案：(65)B；(66)C。

解　析：IEEE 802.11 定义了两种无线网络的拓扑结构，一种是基础设施网络，另一种是特殊网络(Ad Hoc Networking)。在基础设施网络中，无线终端通过接入点访问骨干网设备，或者相互访问。Ad Hoc 网络是一种点对点连接，不需要有线网络和接入点的支持，以无线网卡连接的终端设备之间可以直接通信。

IEEE 802.11g 是 IEEE 802.11 委员会 2003 年制定的物理层标准，它工作在 2.4 GHz ISM 频段上，客户端以 802.11b 的速率在 802.11b APs 上运行，以 802.11g 的速率在 802.11g APs 上运行，最大数据传输速率为 54 Mb/s。

(67) 答　案：D。

解　析：在建筑群布线子系统所采用的铺设方式中，能够对线缆提供最佳保护的方式是地下管道布线，所以选 D。

(68)和(69) 答　案：(68)D；(69)A。

解　析：金融系统涉及银行、众多储户的资产信息，数据重要、敏感，数据量庞大，必须保证数据的绝对安全，同时要保证系统较小的响应时间、很高的服务成功率，而且服务要完整、不间断，故障恢复能力强，整个系统要具有非常高的可用性和可靠性，并不追求采用先进的技术。另外，一般金融系统都是封闭运行的，开放性也不需要放在优先考虑的地位。因此在进行有关金融业务系统的网络设计时，高可用性是首要考虑的问题。

在进行企业网络的需求分析时应该首先进行企业的业务和应用分析，因为网络建设是企业应用的基础，网络系统要向企业的应用系统提供良好的服务，企业的应用需求是设计网络系统的重要依据。

(70) 答　案：A。

解　析：在网络分级设计模型中，核心层的主要功能是尽可能地进行数据交换，在核心层中不应该被牵扯到耗时的数据包操作或任何减慢数据交换的处理，答案选 A。选项 C 是接入层的功能，选项 D 是由汇聚层完成的。

(71)～(75)答　案：(71)C；(72)B；(73)C；(74)A；(75)C。

参考译文：网络访问控制(NAC)的作用是限制对网络的访问，只允许注册的终端和认证的用户访问网络。然而 NAC 不是一个完整的 LAN 安全解决方案，另外还要实现一些主动的或被动的安全手段。Nevis 是第一个也是仅有的全面 LAN 安全解决方案，它以 10Gb/s 的速率对每一个分组进行深度的安全处理，在提供高级别安全的同时能保证网络应用的可利用性和适当的性能。Nevis 集成了 NAC 作为 LAN 的第一道安全防线。此外，企业还需要实现基于角色的网络访问控制以及起关键作用的主动安全测试——实施的多级安全威胁检测和微秒级的安全威胁堵截。集中的安全策略配置、管理和报告使其能够迅速地对问题进行分析，对用户的活动进行跟踪，这些都是实时可见的，也是历史可查的。

下午科目答案与解析

试题一

答　案：

【问题 1】

(1) A 或单模光纤

(2) 要点：传输速率千兆，距离超过 550 m

【问题 2】

(3) A 或核心交换机端口

(4) E 或防火墙 DMZ 端口

(5) B 或核心交换机镜像端口

(6) VOD 服务

【问题 3】

(7) 192.168.110.126

(8)～(10)正确答案有 4 种组合，每种组合均正确。

组合 1：

(8) 192.168.110.129～192.168.110.190

(9) 192.168.110.193～192.168.110.222

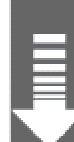
(10) 192.168.110.225～192.168.110.254

组合 2：

(8) 192.168.110.129～192.168.110.190

(9) 192.168.110.225～192.168.110.254

(10) 192.168.110.193～192.168.110.222



组合 3：
(8) 192.168.110.193～192.168.110.254
(9) 192.168.110.129～192.168.110.158
(10) 192.168.110.161～192.168.110.190
组合 4：
(8) 192.168.110.193～192.168.110.254
(9) 192.168.110.161～192.168.110.190
(10) 192.168.110.129～192.168.110.158
(11) 255.255.255.128
(12) 255.255.255.192
(13) 255.255.255.224
(14) 255.255.255.224

解　析：

【问题 1】

按照千兆以太网的规范，使用双绞线的传输距离是中间的线缆长度+两端的跳线长度不能超过 100 m；同轴电缆在千兆传输时能够达到 25 m 的距离；而多模光纤，千兆数据通信的距离规范为 220～550 m，其中当使用的光纤核心直径是 62.5 μm 时，通信距离为 220 m，光纤核心直径是 50 μm 时，通信距离为 550 m；对于单模光纤而言，在千兆传输时最大连接距离可达 5 km，按照题目要求网络中心与图书馆相距 700 m，而且两者之间采用千兆连接，那么两个楼之间的通信介质应选择单模光纤。

【问题 2】

服务器在进行部署时应充分考虑到功能、服务提供对象、流量和安全等因素。按照题目要求，VOD 服务对校内提供服务，且其流量较大，应部署在核心交换机端口。而 Web 服务器需对外提供服务，一般部署在防火墙 DMZ 端口。网络流量监控需要监听交换网络中所有流量，但是通过普通交换机端口去获取这些流量有相当大的困难，因此需要通过配置交换机来把一个或多个端口的数据转发到某一个端口来实现对网络的监听，这个端口就是镜像端口，而网络流量监控服务器需要部署在镜像端口。

【问题 3】

在进行 IP 地址部署时，由于要求各部门处于不同的网段，这样就要求在给定的网段内划分地址。由题目可知，教师机房起始地址为 192.168.110.0，主机数量为 100 台，因此其子网掩码为 255.255.255.128，可用地址为 192.168.110.1～192.168.110.126；教研室 A 分配的 IP 地址不能少于 32 个可用地址，因此其子网掩码为 255.255.255.192；教研室 B、教研室 C 的可用地址不能少于 20 和 25 个，因此其子网掩码为 255.255.255.224。其中，只有教师机房的起始地址固定，其他的可组合分配。

试题二

答　案：

【问题 1】(1) C　(2) B
【问题 2】(3) B　(4) D
【问题 3】(5) A

【问题4】(6) A (7) B

【问题5】(8) C

【问题6】(9) 授权访问 (10) 200.115.12.0～200.115.12.127

解 析：本题考查的是对FTP服务器的配置。主要是Windows图形界面下对FTP服务器的配置，如FTP服务器的目录、端口、访问控制、匿名访问与授权访问形式、本地账户的建立等。

【问题1】

由于架设FTP站点需要IIS 6.0的支持，而在默认状态下Windows Server 2003服务器并没有安装该组件，所以在架设具有用户隔离功能的FTP站点之前，需要安装好IIS 6.0组件，并将其中的“隔离用户”FTP组件一并安装成功。下面就是安装“隔离用户”FTP组件的具体操作步骤。

(1) 在Windows Server 2003服务器系统中，依次选择“开始”→“设置”→“控制面板”命令，在弹出的“控制面板”窗口中单击“添加或删除程序”图标，在其后出现的“添加或删除程序”设置界面中单击“添加/删除 Windows 组件”按钮，进入到一个标题为“Windows组件向导”的界面。

(2) 在“组件”列表框中，选中“应用程序服务器”复选框，并单击“详细信息”按钮，在随后弹出的“应用程序服务器”设置窗口中，单击其中的“Internet信息服务”选项，进入到“Internet 信息服务”对话框，在该对话框的子组件列表中选择“文件传输协议(FTP)服务”选项，单击“确定”按钮即可。

【问题2】

该题考查用户在同一个IP地址下配置两个不同FTP服务的配置过程。

由于安装FTP服务的主机只有一个静态公网IP地址200.115.12.3，因此所有FTP服务的IP地址均应该配置为该IP地址。而FTP服务默认配置的端口号为21，由于此时安装的默认FTP服务已经使用了21端口号，为了避免冲突，应该使用系统尚未使用的其他端口号。

【问题3】

本题考查FTP服务安装的默认主目录。在Windows操作系统下安装FTP服务会默认保存在C:\ftp\root目录中。

【问题4】

为了防止普通用户通过匿名账号访问FTP站点，我们在架设FTP站点的时候肯定会限制匿名账号的访问权限，只让特定用户访问FTP站点中的内容。为此，在正式架设FTP站点之前，有必要在Windows Server 2003服务器系统中为FTP站点创建一些用户访问账号，此后用户必须凭事先创建好的账号才能登录进FTP站点。可以为那些需要访问FTP站点的所有用户都创建一个账号信息。

当创建好了用户访问账号后，下面需要进行的操作就是在服务器系统的本地硬盘中创建好FTP站点的主目录，以及各个用户所对应的用户账号，以便确保每一个用户此后只能访问自己的目录，而没有权限访问其他用户的目录。

为了让架设好的FTP站点具有用户隔离功能，必须按照一定的规则设置好该站点的主目录及用户目录。首先需要在NTFS格式的磁盘分区中建立一个文件夹，例如该文件夹名称为aaa，并把该文件夹作为待建FTP站点的主目录。



接着进入到 aaa 文件夹窗口中，并在其中创建一个子文件夹，同时必须将该子文件夹的名称设置为 Local User(该子文件夹名称不能随意设置)。再打开 Local User 子文件夹窗口，然后在该窗口下依次创建好与每个用户账号名称相同的个人文件夹。如果用户账号名称与用户目录名称不一样的话，用户就无法访问到自己目录下面的内容。

做好上面的准备工作后，就能正式搭建具有“用户隔离”功能的 FTP 站点了。因此(6)、(7)的答案分别为 A、B。

【问题 5】

要是希望架设成功的 FTP 站点具有匿名登录功能的话，那就必须在 Local User 文件夹窗口中创建一个 Public 子目录，以后访问者通过匿名方式登录进 FTP 站点时，只能浏览到 Public 子目录中的内容。

【问题 6】

如果公司只允许 IP 地址段 200.115.12.0/25 上的用户访问“内部 FTP 站点”，应该进行如下配置。

在图 14.7 所示的对话框中：

(1) 选中“授权访问”单选按钮，这样会接受在特定地址范围内的主机访问；

(2) 单击“添加”按钮，即打开如图 14.8 所示的对话框。

在图 14.8 所示的对话框中：

(1) 选中“一组计算机”单选按钮；

(2) 在“IP 地址”文本框中填入地址：200.115.12.0～200.115.12.127 中的任意一个即可，然后在“子网掩码”文本框中输入 255.255.255.128；

(3) 单击“确定”按钮结束配置。

试题三

答　案：

【问题 1】(1) B 或分布式数据库　(2) A 或 C/S　(3) A 或 named

【问题 2】(4) C　(5) A　(6) B

【问题 3】(7) master　(8) 222.35.40.0　(9) /var/named

解　析：

【问题 1】

在 TCP/IP 网络系统中使用的 IP 地址和主机名的转换机制是 DNS，它使用一种分层的分布式数据库来处理地址和名字的转换，转换信息分布在一个层次结构的若干台域名服务器上。

在 Linux 中，域名服务(DNS)是由 BIND 软件实现的。BIND 是一个 C/S 系统，其客户端称为转换程序(resolver)，它负责产生域名信息的查询，并将这类信息发送给服务器。BIND 的服务器端是一个称为 named 的守护程序，负责回答转换程序的查询。

【问题 2】

DNS 客户在向 DNS 系统查询主机 IP 地址时，首先构造名字查询报文，然后根据客户机在网络配置中指定的 DNS 服务器地址，将查询报文发送给 DNS 服务器。DNS 服务器有两种处理模式：一种是递归查询，当收到 DNS 工作站的查询请求后，若本地 DNS 服务器查询成功则返回客户端查询结果，若本地查询失败，由本地域名服务器利用服务器上的软

件采用递归算法请求下一个服务器(将查询请求向下一个 DNS 服务器转发)，并将结果返回查询客户；另一种是迭代查询，当收到 DNS 工作站的查询请求后，如果 DNS 服务器中没有查到所需 IP 地址，该 DNS 服务器将告知另外一台 DNS 服务器的 IP 地址，然后再由 DNS 工作站自行向此 DNS 服务器查询，直到查到所需信息为止(或者失败)。一般在 DNS 服务器之间的查询请求属于迭代查询。

【问题 3】

在多个 zone 语句中定义区域文件，指出某个域的地址转换配置信息(或者反向转换配置信息)存放的数据库文件名称和类型时，如果为特定的域设置多个名字服务器，可以使用 type master 选项只设置其中一个为主要的或授权名字服务器，其他名字服务器(个数不限)必须设置为从名字服务器(type slave)。反向 DNS 区域(通过 IP 地址查询主机名称为反向查询，查询信息在反向 DNS 区域文件中)配置采用特殊的区域名字，要求把网络 IP 地址的分段数字“反向”，并在名字的最后加 in-addr.arpa，该文件的数字串(用点符号分隔)从右到左就是由该区域文件管理网络域的网络地址。

试题四

答　案：

【问题 1】(1) A　(2) CNAME

【问题 2】

存在的主要问题：不能区分服务器的差异，也不能反映服务器的当前运行状态(负载量的大小)；或者，不能根据负载情况实现动态调度。

如果一个服务器发生故障不可访问，会造成混乱，一些人能够访问 WWW 服务，另一些则不可以。

【问题 3】(3) false(或 0)　(4) test.com　(5) 192.168.1.10　(6) 192.168.1.3　(7) 192.168.1.0　(8) 255.255.255.255

【问题 4】

NFS(网络文件系统)服务器由主机 ns 担任，Web 服务器(www1 和 www2)作为它的客户，共享其数据和服务脚本，保证了 Web 服务的数据同步或一致。

NFS 服务器需要向 www1 和 www2 分发数据文件，为避免分发和同步占用 Web 服务的带宽，左边的交换机组成 192.168.2.0 NFS 专用局域网，以保证 Web 的服务质量。

同时这种配置将使 NFS 文件系统对外界不可用，增强了服务器的安全性。

解　析：本题主要考查服务器集群与负载均衡技术，以 Web 服务器为例。考查了 DNS 服务器的配置及 DNS 的循环机制的优点与不足，还考查了 Linux 下基础网络参数的配置。最后对 NFS 网络文件系统的相关概念以简答的方式进行考查。

【问题 1、2】采用多个服务器组成“集群”不仅能够提高整个系统的可靠性，而且还能够分担系统负载(负载均衡)。

应用循环 DNS 配置技术可以实现不能动态调整的、简单的负载均衡技术，具体来讲就是通过恰当配置 DNS 区域文件，将两台不同 IP 地址的服务器，利用“别名”机制关联到一个统一的主机名上，客户通过这个统一的主机名访问服务器资源时，DNS 名称服务器将依次给出第一个服务器的 IP 地址、第二个服务器的 IP 地址、第一个服务器的 IP 地址……这样不间断地循环。循环 DNS 配置的缺点之一是，名称服务器没有办法知道哪台服务器负载



重，如果一台服务器崩溃或由于某种原因不可用了，循环 DNS 仍将返回不可用的服务器的 IP 地址，使有些用户能够访问成功而有些用户访问不成功。

【问题 3】采用基于硬件(导向器)的负载均衡方法能够克服循环 DNS 配置的缺点。图中 WSD Pro 导向器拦截了所有访问服务器资源的通信连接，根据一种或多种算法选择一台服务器(物理上的)将连接进行转发，比如导向器可以根据服务器的“忙碌”情况来选择，即导向器可以利用网络和服务的可用性即服务器的性能来选择某个服务器为客户提供服务。

【问题 4】采用基于硬件(导向器)的负载均衡方法能够克服上述缺点。不过采用上述方法实施负载均衡还需要解决服务器之间的数据同步等关键问题，必须有另外一种机制来保证不同的服务器对外提供的服务是一致的。在第三台服务器上(本题中是 DNS 服务器)安装 NFS 系统是可行的解决方案，可在该服务器上一个或多个磁盘中安装，Web 服务器通过 NFS 可以共享访问这些磁盘。但是应该看到，采用这种方法工作效率会较低，而且存在单点故障。NFS 服务器的 eth0 网卡的地址是 192.168.1.3，其/etc/sysconfig/network 文件内容如下。

```
NETWORKING=yes
FORWARD_IPV4=0
HOSTNAME=ns.test.com
DOMAINNAME=test.com
GATEWAY=192.168.1.10
GATEWAYDEV=eth0
```

/etc/sysconfig/network-scripts/ifcfg-eth0 文件内容如下：

```
DEVICE=eth0
IPADDR=192.168.1.3
NETMASK=255.255.255.0
NETWORK=192.168.1.0
BROADCAST=255.255.255.255
ONBOOT=yes
```

NFS 服务器需要向 www1 和 www2 分发数据文件，为避免分发和同步占用 Web 服务的带宽，左边的交换机组成 192.168.2.0 NFS 专用局域网，以保证 Web 的服务质量。

同时这种配置将使 NFS 文件系统对外界不可用，增强了服务器的安全性。

试题五

答　案：

【问题 1】(1) 修改主机名为 SwitchA　(2) 进入 VLAN 配置子模式　(3) 设置本交换机为 Server 模式　(4) 设置域名为 vtpserver　(5) 启用修剪功能

【问题 2】(6) mode trunk　(7) vlan all

【问题 3】(8) switchport mode access　(9) switchport access vlan 10

【问题 4】(10) 128　(11) e0/3

解　析：本题考查交换机配置、基于端口权值的负载均衡配置。

【问题 1】

本题考查的是交换机的基本配置知识。

【问题 2】

本题考查的是交换机的 Trunk 配置。

【问题 3】

本题考查的是将端口划入 VPN 的基本操作。

【问题 4】

本题考查的是端口权值的负载均衡配置。

默认情况下端口权值为 128，STP 协议可以根据权值的大小来使用不同 Trunk 发送和接收不同 VLAN 的数据，从而实现负载均衡的目的。

按照题目中的配置，VLAN20 在端口 3 的权值为 10，在其他端口的权值为默认值。故 VLAN20 的数据通过 SwitchA 的端口 3 收发数据。

14.2.2　考前模拟卷 2 参考答案与解析

上午科目答案与解析

(1)和(2)答案：(1)C；(2)B。

解　析：如果按照串行方式执行指令，则每条指令都需 3 步才能执行完。100 条指令的执行时间为：

$$(4\Delta t+3\Delta t+5\Delta t)\times 100=1200\Delta t$$

如果按照流水线方式执行时，执行完 100 条指令需要的时间为：

$t_{取指}+\max\{t_{分析}，t_{取指}\}+98\times\max\{t_{取指}，t_{分析}，t_{执行}\}+\max\{t_{分析}，t_{执行}\}+t_{执行}$

$=4\Delta t+4\Delta t+490\Delta t+5\Delta t+5\Delta t$

$=508\Delta t$

(3) 答　案：B。

解　析：在页式存储管理中，逻辑地址为页内地址。本题中，页面的大小为 8 KB，则页内有效地址的范围为 0～8191。本题中逻辑地址为 9612，则有效地址为 9612 除以 8192 取余为 1420。由题目中的地址变换过程图可知，逻辑地址 9612 在第 1 页，该页在内存中对应的物理块号为 3，因此，可以计算物理地址 a 为 8192×3+1420=25 996。

(4) 答　案：C。

解　析：构成计算机控制器的部件主要有指令寄存器(IR)、程序计数器(PC)、程序状态寄存器(PSW)、时序产生器和微操作信号发生器等。算术逻辑单元(ALU)不是构成控制器的部件，而是属于运算器的部件。

(5) 答　案：C。

解　析：从可靠性设计角度分析，该试题给出的是一种串并混合系统。首先考虑部件 2 和部件 3 是并联冗余结构，它们的可靠度分别为 0.70，两者并联冗余的可靠度为 $1-(1-0.70)^2=0.91$。在此基础上，系统可以看作是可靠度为 0.90 的部件 1、可靠度为 0.91 的冗余部件和部件 4 串联构成，串联系统的可靠度为各部件可靠度之积，要求构成的系统的可靠度不低于 0.75。若设部件 4 的可靠度为 R_4，则

$$0.9\times(1-(1-0.70)^2)\times R_4=0.75$$

从而可以由下式求出部件 4 的可靠度：



$$R_4=\frac{0.75}{0.9\times[1-(1-0.7)^2]}$$

(6) 答　案：C。

解　析：通常，原型是指模拟某种产品的原始模型。在软件开发中，原型是软件的一个早期可运行的版本，它反映最终系统的部分重要特性。使用原型的原型化方法特别适用于需求不确定性较高的软件系统的开发。它的基本思想是根据用户给出的基本需求，通过快速实现构造出一个小型的可执行的模型，满足用户的基本要求，这就是系统界面原型。让用户在计算机上实际运行这个用户界面原型，在试用的过程中得到亲身感受和受到启发，做出反应和评价，提出同意什么和不同意什么，然后开发者根据用户的意见对原型加以改进。随着不断试验、纠错、使用、评价和修改，获得新的原型版本，如此周而复始，逐步减少分析和通信中的误解，弥补不足之处，进一步确定各种需求细节，适应需求的变更，从而提高最终产品的质量。

(7) 答　案：A。

解　析：CMM 将软件过程改进的进化步骤组织成 5 个成熟度等级，即初始级、可重复级、定义级、管理级和优化级。这 5 个成熟度等级定义了一个有序的尺度，用来测量一个组织的软件过程成熟度和评价其软件过程能力，为不断改进过程奠定了循序渐进的基础。初始级对软件过程几乎没有明确定义的步骤，杂乱无章；可重复级建立了基本的项目管理过程来跟踪成本、进度和机能；在定义级，管理和工程的软件过程已经文档化、标准化，并综合成整个软件开发组织的标准化过程；管理级对软件过程与产品质量建立了定量的质量目标，制定了软件过程和产品质量的详细的度量标准；优化级加强了定量分析，不断持续地改进软件过程。

(8) 答　案：A。

解　析：目前市场上的各类软件开发工具十分丰富，价格相差很大，在评价和选择软件开发工具时，可以根据功能、易用性、稳健性、硬件要求和性能、服务和支持等标准来衡量软件开发工具的优劣。易维护性、可移植性和可扩充性都是开发软件时应当考虑的问题。

(9) 答　案：D。

解　析：本题图中有 3 条任务流，任务流①→②→③→⑤→⑥，所需时间为 16 天；任务流①→②→③→④→⑤→⑥，所需时间为 20 天；任务流①→②→④→⑤→⑥，所需时间为 17 天。由此可知关键路径是①→②→③→④→⑤→⑥，工期为 21 天。

(10) 答　案：B。

解　析：《计算机软件保护条例》第二十八条规定，软件复制品的出版者、制作者不能证明其出版、制作有合法授权的，或者软件复制品的发行者、出租者不能证明其发行、出租的复制品有合法来源的，应当承担法律责任。“盗版软件”即侵权的软件复制品。

《计算机软件保护条例》判断侵权是以软件侵权复制品持有人主观上知道(或者应当知道)所持软件是否为侵权复制品为标准。知道软件是侵权复制品而使用运行，应当承担法律责任；主观上不知软件是侵权复制品，对软件的使用运行等行为不承担侵权责任。题目中，盗版软件持有者并不知道软件是盗版的，因此其不必承担侵权责任。

(11) 答　案：C。

解　析：根据 Nyquist 定理可知，信道支持的最大数据速率 $R=B\log_2N=2W\log_2N=2\times4$ KB$\times\log_2 4=16$ Kb/s。

(12) 答　案：D。

解　析：光纤的芯线由纯净的玻璃或塑胶材料制成。包层包围着芯线部分，它也是玻璃或塑料的，但它的光密度要比核心部分低，亦即包层的折射率比芯线的折射率低。进入光纤的光波在两种材料的界面上形成全反射，从而不断地向前传播。在多模光纤中，光波在光导纤维中以多种模式传播，不同的传播模式有不同的电磁场分布和不同的传播路径，而单模光纤只以一种模式传播。相对于单模光纤来讲，多模光纤的模间色散较大，带宽比较窄，数据传输速率较低。

(13) 答　案：B。

解　析：差分曼彻斯特编码是一种双相码，它又是一种差分码，0 位的前沿有相位变化，1 位的前沿没有相位变化，由此可以判断选项 B 的图形是差分曼彻斯特编码。选项 A 中，用高电平到低电平的转换表示 1，而用低电平到高电平的转换表示 0，这是曼彻斯特编码。选项 C 中，每一位中都有一个电平转换，这是一种双相码，但不是曼彻斯特码，也不是差分曼彻斯特码。选项 D 中用高电平表示 0，低电平表示 1，这是极性码。

(14) 答　案：C。

解　析：由题意可知，每个字符共 10 位，则数据速率为 10×100=1000 b/s，而其中数据位为 7 位，可知有效的数据速率为

$$\frac{7}{1+7+1+1}\times1000=700\text{ b/s}$$

(15) 答　案：B。

解　析：光纤线路的多路复用美国标准为同步光纤网络(SONET)，该标准又被划分为多个级别，其中级别 OC-3 的数据速率为 155 Mb/s，级别 OC-1 的数据速率为 51 Mb/s，级别 OC-12 的数据速率为 622 Mb/s，级别 OC-48 的数据速率为 2488 Mb/s。

(16)和(17)答　案：(16)B；(17)B。

解　析：E1 载波把 32 个 8 位一组的数据样本组装成 125 μs 的基本帧，每个子信道的数据速率为 8b/125 μs=64 Kb/s。32 个子信道中，30 个用于传送话音数据，两个用于传送控制信令，则控制开销占 2/32=6.25%。

(18) 答　案：B。

解　析：运算过程如下。①因为生成多项式 $G(x)$的阶数是 5，所以先将信息码字后加 5 个 0，得到 1110001100000；②用生成多项式 $G(x)$对应的二进制序列 110011 模 2 除以上述二进制序列，得到余数为 11010，故答案选 B。

(19) 答　案：A。

解　析：数字用户线路 DSL 按数据传输的上、下行传输速率的相同和不同，分为对称和非对称两种传输模式。对称 DSL 技术中，上、下行传输速率相同，代表有 HDSL、SDSL 等。非对称 DSL 技术的上、下行传输速率不同，主要有 ADSL、RADSL、VDSL 等。

(20) 答　案：D。

解　析：基本速率接口由两个 64 Kb/s 的 B 信道和一个 16 Kb/s 的 D 信道组成。B 信道可用于承载数字数据、PCM 编码数字语音等，D 信道可传输低速率数据，也可用以传输



信令。

基群速率接口也称一次群速率接口，即(30B+D)。B 和 D 均为 64 Kb/s 的数字信道。B 信道主要用于传输用户信息流；D 信道主要用于传送电路交换的信令信息，也用于传送分组交换的数据信息。基群速率接口由 30 个 64 Kb/s 的 B 信道和一个 16 Kb/s 的 D 信道组成。

(21) 答　案：B。

解　析：集线器 Hub 属于一层设备，网桥和交换机属于二层设备，路由器属于三层设备。二层设备可能分割冲突域，三层设备可能分割广播域。在选项 A 中，P、Q 中间有二层设备网桥，不在同一个冲突域中，但在同一个广播域中；选项 C 中，Q、R 中间只有一个一层设备 Hub，既在同一个广播域中，也在同一个冲突域中；选项 D 中，S、T 中间有二层设备交换机，不在同一个冲突域中，但在同一个广播域中。选项 B 中，P 和 S 被一台三层设备路由器隔开，属于不同的广播域，它们之间不能通过 IP 全局广播分组，因此答案为 B。

(22) 答　案：C。

解　析：Internet 协议要满足一定的封装关系，上传协议封装在下层协议数据单元中传送。应用层协议 HTTP 和 TELNET 是通过 TCP 连接发送，SNMP 和 TFTP 是利用 UDP 数据报传送。

(23)和(24) 答　案：(23)C；(24)C。

解　析：为了确保连接建立和终止的可靠性，TCP 使用三次握手法。所谓三次握手法就是在连接建立和终止过程中，通信的双方需要交换 3 个报文。这种建立连接的方式可以防止产生错误的连接。产生错误连接的主要因素来源于网络失效期间存储在网络中的连接请求，这些过期连接请求在网络故障恢复后可能继续到达目标端，干扰新发出的连接请求，从而建立错误的连接。在创建一个新的连接过程中，三次握手法要求每一端产生一个随机的 32 位初始序列号，由于每次请求新连接的初始序列号不同，因此，TCP 可以将过期的连接区分开来，避免二义性的产生，从而保证连接的正确性。

(25) 答　案：B。

解　析：在 Ethernet II 格式中，一个帧的最大长度是 1518 字节，而帧头占 14 字节，帧尾占 4 字节，IP 头最少 20 字节，TCP 头最少 20 字节，因此 TCP 段中的数据部分最长为 1518−14−4−20−20=1460 字节，答案选 B。

(26) 答　案：B。

解　析：ARP 是地址解析协议的简称，用于将 IP 地址解析成 MAC 地址。这是因为在实际通信中，物理网络依然是利用 MAC 地址进行报文传输，IP 地址在物理网络中是不能识别的，因此必须建立 IP 地址和 MAC 地址之间的映射关系，这一过程称为地址解析。通过 ARP 协议可以在 Cache 的 ARP 表中存储 IP 地址及经过解析的 MAC 地址。

(27) 答　案：C。

解　析：OSPF 是一种基于 Dijkstra 算法的链路状态协议，这种协议要求路由器掌握完整的网络拓扑结构，并据此计算出到达目标的最佳路由。该算法的基本思想是互联网上的每个路由器周期性地向其他路由器广播自己与相邻路由器的连接关系，利用其他路由器的广播信息，互联网上的每个路由器都可以形成一张由点和线连接而成的抽象拓扑结构图；一旦得到了这张图，路由器就可以按照 Dijkstra 算法计算出以本地路由器为根的 SPF 树，通过这棵树路由器就可以生成自己的路由表。

(28) 答　案：B。

解　析：水平分割的方法规定，路由器必须有选择地将路由表中的信息发送给邻居，而不是向邻居发送整个路由表。具体来说，一条路由信息不会被发送给该信息的来源方向。

简单的水平分割方案是不把从一个邻居学习到的路由发送给那个邻居，带有反向毒化的水平分割方案是把从一个邻居学习到的路由设置为无限大，再发送给那个邻居。

(29) 答　案：A。

解　析：边界网关协议(Border Gateway Protocol，BGP)是一种外部网关协议，用于自治系统之间的路由器交换路由信息。

自治系统内部的路由器之间交换路由信息要使用内部网关协议，OSPF 和 RIP 等属于内部网关协议。

Internet 主干网的路由器之间利用核心网关协议(Gateway to Gateway Protocol，GGP)交换路由信息。

(30)和(31) 答　案：(30)B；(31)A。

解　析：POP3 是邮局协议 POP 的第 3 个主要版本，它允许用户通过 PC 动态检索邮件服务器上的邮件。POP3 协议采用客户机/服务器(Client/Server)模式，其客户机运行在用户的 PC 上，当用户需要下载邮件时，客户机向 POP 服务器的 TCP 端口 110 发送连接请求，当 TCP 连接建立成功后，POP 客户机就可以向服务器发送命令，下载和删除邮件。

(32) 答　案：D。

解　析：

vlan-menbership static vlan_ID 为 Cisco1900 交换机端口分配 VLAN，后面必须说明端口号。

vlan database 用于从特权模式进入 VLAN 配置模式。

switchport mode access 将端口设置为接入链路连接。

switchport access vlan 1 将当前端口划分在 1 号 VLAN 中。因此答案为 D。

(33) 答　案：C。

解　析：路由器是一种网络层转发设备，它必须分拆数据帧，识别 IP 数据报中的目标地址字段，然后进行转发。它处理的信息量比交换机多，处理速度比交换机慢，因此选项 A 错误。路由器可以实现不同的服务质量，根据 IP 报头中 ToS 字段的编码选择不同可靠性、优先级、延迟或吞吐率的线路进行转发，所以不只是提供延迟最小的路由，可见选项 B 错误。不但能根据逻辑地址进行转发，而且可以根据物理地址进行交换的设备叫三层交换机，不是路由器，因此选项 D 错误。

(34) 答　案：D。

解　析：配置路由器端口应在全局状态下输入 interface <端口号>，进入端口配置状态。全局配置模式的提示符是R1 (config)#，端口配置模式的提示符是R1 (config-if)#。

(35) 答　案：C。

解　析：在用户命令或特权命令状态下，show ip route 命令显示路由信息，show ip protocol 命令显示配置的路由协议。

(36) 答　案：C。

解　析：在 Linux 操作系统中，/etc/hostname 文件包含了 Linux 系统的主机名称，包括完全的域名；/etc/host.conf 文件指定如何解析主机域名，Linux 通过解析库来获得主机名对

应的 IP 地址；/etc/resolv.conf 文件负责配置 DNS，它包含了主机的域名搜索顺序和 DNS 服务器的地址。

(37) 答　案：C。

解　析：/etc/passwd 文件是 Linux 系统中用于用户管理的重要文件，这个文件对所有用户都是可读的，Linux 系统中的每个用户在/etc/passwd 文件中都有一行对应的记录，用户在登录时，会先在/etc/passwd 文件中找到用户 ID。/etc/shadow 保存着加密后的用户口令。/etc/group 是管理用户组的基本文件，在/etc/group 中每行记录对应一个组，它包括用户组名、加密后的组口令、组 ID 和组成员列表。

(38) 答　案：A。

解　析：Linux 系统对文件的访问设定了 3 级权限，分别是文件所有者、与文件所有者同组的用户和其他用户；同时对文件的访问做 3 种处理操作，即读取、写入和执行。Linux 文件被创建时，文件所有者可以对该文件的权限进行设置。默认情况下，系统将创建的普通文件的权限设置为-rw-r-r-。

(39)和(40) 答　案：(39)B；(40)D。

解　析：Windows 的活动目录逻辑单元包括组织单元(OU)、域、域树和域森林，它们构成了层次的结构，域森林由域树组成，域树又由域组成，域中的对象可以按 OU 划分。OU 负责把对象组织起来。

安装活动目录要求分区的文件系统为 NTFS。

(41)和(42) 答　案：(41)A；(42)D。

解　析：在配置 IIS 时，如果想禁止某些 IP 地址访问 Web 服务器，应在“默认 Web 站点属性”对话框中“目录安全性”选项卡的“IP 地址及域名限制”选项组中配置。在配置 IIS 的发布目录时，可以将其配置在本机目录上、联网的其他计算机共享目录上以及重定向到 URL 上。

(43) 答　案：B。

解　析：在 Windows 操作系统中，Web 服务器只能安装一套 IIS 系统，使用虚拟目录和多个 Web 服务端口可以实现多个网站的发布，但是其域名是相同的，而使用虚拟主机可以实现一台具有多个域名的 Web 服务器。

(44) 答　案：B。

解　析：PGP 是一个完整的电子邮件安全软件包，包括加密、鉴别、电子签名和压缩等技术；IPSec 是在 IP 包级为 IP 业务提供保护的安全协议标准；DES 是一种常用的对称加密算法，答案选 B。

(45) 答　案：D。

解　析：包过滤防火墙根据定义好的过滤规则审查每个数据包并确定数据包是否与过滤规则匹配，从而决定数据包是否能通过。

(46) 答　案：B。

解　析：多形病毒是一种较为高级的病毒，这种病毒在每次感染后会改变自己，使得不可能通过病毒的“签名”来检测自己。

(47)和(48) 答　案：(47)D；(48)C。

解　析：数据加密标准(DES)是一种分组加密算法，输入、输出块均为 64 位，因此(47)

的答案选 D。

DES 使用的密钥为 64 位，其中实际密钥长度为 56 位，有 8 位用于奇偶校验，因此，(48)的答案选 C。

(49)和(50) 答　案：(49)B；(50)C。

解　析：SNMP 协议实体发送请求和应答报文的默认端口号是 161，SNMP 代理发送陷入报文(Trap)的默认端口号是 162。

(51) 答　案：C。

解　析：tracert 命令的用法如下。

```
tracert [-d] [-h maximum_hops] [-j hop_list] [-w timeout] <target_name>
```

其中：

-d 表示不进行名字解析，显示中间节点的 IP 地址。

-h maximum_hops 指定了最大跟踪跳步数。

-j hop_list 指定了有限源路由。

-w timeout 说明了等待 ICMP 回声响应报文的时间。

target_name 是用 IP 地址或主机名表示的目标。

(52) 答　案：D。

解　析：SNMP 定义应用层协议，它依赖于 UDP 数据报服务。之所以选择 UDP 协议而不是 TCP 协议，是因为 UDP 效率较高，这样实现网络管理不会太多地增加网络负载。但由于 UDP 不可靠，所以 SNMP 报文容易丢失。为此，对 SNMP 的实现是将每个管理信息装配成单独的数据包独立发送，而且报文较短，不超过 484 个字节。

(53) 答　案：D。

解　析：在一般情况下，网络上所有的计算机都可以接收到通过的数据帧，但对不属于自己的报文则不予响应。但是如果某工作站的网络接口处于混杂模式，那么它就可以捕获网络上所有的报文和帧，如果一个工作站被配置成这样的方式，它就是一个嗅探器。

(54) 答　案：C。

解　析：用于本地环路(Loopback)的 IP 地址是 127.0.0.1，通过这个地址可以检测主机 TCP/IP 协议的配置。10.10.10.1 是一个私网地址；255.255.255.0 是一个子网掩码；192.0.0.1 是一个普通的 C 类地址。

(55)和(56) 答　案：(55)D；(56)A。

解　析：网络 176.16.1.12/20 的子网掩码为 11111111 11111111 11110000 00000000，即 255.255.240.0，其中的主机地址为 12 位，有 $2^{12}-2=4094$ 个主机地址。

(57) 答　案：D。

解　析：私网 IP 地址包括以下 3 组。

1 个 A 类网络 10.0.0.0～10.255.255.255。

16 个 B 类网络 172.16.0.0～172.31.255.255。

256 个 C 类网络 192.168.0.0～192.168.255.255。

只有选项 D 中的 IP 地址属于 B 类私网地址。

(58) 答　案：C。



解　析：地址 172.16.2.12/24 的二进制表示为 10101100 00010000 00000010 00001100，子网掩码为 24 位，所以网络地址为 10101100 00010000 00000010 00000000，即 172.16.2.0。

(59) 答　案：A。

解　析：这 4 个路由的前 16 位相同，因此只需要观察它们的第 3 段。

193=(**11000**001)$_2$

194=(**11000**010)$_2$

196=(**11000**100)$_2$

198=(**11000**110)$_2$

可见第 3 段的前 5 位相同。因此可知 10.1.193.0/24、10.1.194.0/24、10.1.196.0/24 和 10.1.198.0/24 这 4 条路由的前 21 位相同，汇聚后的地址是 10.1.192.0，故答案选 A。

(60) 答　案：A。

解　析：VLAN ID 用 12 位表示，即数值范围为 1～4096。其中 1～1005 是交换机支持的标准范围。1 是默认的 VLAN，一般用于设备管理，只能使用，不能删除。

(61) 答　案：B。

解　析：在 VLAN 中，属于同一个 VLAN 的所有端口构成一个广播域，同一个广播域的 VLAN 成员可以直接通信。但不同的 VLAN 之间不能直接通信，必须通过第三层路由功能完成，可由路由器或第三层交换机实现。在第三层交换机中增加了一个第三层交换模块，由该模块完成路径选择功能。

(62) 答　案：D。

解　析：VTP 是交换机之间共享 VLAN 信息的机制，而路由器之间交换的是路由信息，故选项 A 不正确；选项 B 中，划分 VLAN 的最主要的目的就是抑制广播风暴，不同的 VLAN 之间不需要用网桥分隔，再说网桥是一个二层设备，无法过滤广播信息，也不正确；选项 C 中，虽然 Cisco 交换机的初始状态是工作在 VTP 服务器模式，但其 VTP 域的名称是 NULL，因此无法将其 VLAN 配置信息广播给其他交换机，也不正确；答案选 D。

(63) 答　案：B。

解　析：对于非坚持监听算法，如果监测到信道忙，则后退一个随机时延再监听，从而减少了冲突的概率；但这会使信道的利用率降低，而且增加了发送时延。

对于 1-坚持型监听算法，如果监听到信道忙，继续监听，直到信道空闲后立即发送。这有利于抢占信道，减少信道空闲时间。但是多个站同时都在监听信道时必然发生冲突。

P-坚持型监听算法汲取了以上两种算法的优点。较之非坚持型监听算法，P-坚持型监听算法的信道利用率高，但易冲突。

(64) 答　案：B。

解　析：快速以太网标准 100Base-TX 采用的传输介质是 5 类无屏蔽双绞线(UTP)，TX 表示 Twisted Pair。

(65) 答　案：C。

解　析：在以太网中，最大传输单元(MTU)是 1500 个字节，最大帧长是 1518 个字节。

(66) 答　案：B。

解　析：802.11i 标准是对 WEP 协议的改进。802.11i 定义了新的密钥交换协议 TKIP 和高级加密标准 AES。TKIP 提供了报文完整性检查，每个数据包使用不同的混合密钥，每

次建立连接时生成一个新的基本密钥，这些手段的采用使得诸如密钥共享、碰撞攻击和重放攻击等无能为力，从而弥补了 WEP 协议的安全隐患。

(67) 答　案：C。

解　析：无线路由器是具有路由功能的 AP，一般情况下，它不仅具备无线 AP 的所有功能，而且还包括了网络地址转换功能，因此可利用它建立一个更小范围的无线局域网，实现家庭无线网络中的 Internet 连接共享，实现 ADSL 和小区宽带接入。

(68) 答　案：C。

解　析：在进行网络设计时应充分考虑现有的网络结构，在不影响现有系统正常运行的情况下，逐步完善网络安全系统。

(69) 答　案：A。

解　析：不同的网络服务应用需要有不同的 QoS 要求。QoS 的关键指标包括可用性、吞吐量、时延、时延变化和丢失。ATM 的最大优势在于可以有效地实现 QoS。

(70) 答　案：A。

解　析：在网络分级设计模型中，核心层的主要功能是尽可能地进行数据交换。在核心层中不应该被牵扯到耗时的数据包操作或任何减慢数据交换的处理，因此，应该避免在核心层中使用访问控制列表或数据包过滤之类的功能，这一功能应由汇聚层来完成，答案选 A。

(71)～(75)答　案：(71)B；(72)C；(73)A；(74)D；(75)B。

参考译文：Cookies(小甜饼)最初由 Netscape Communications 提出，它是一种通用机制，这种机制使一个 HTTP 连接的服务端的应用程序，如 CGI、脚本(Script)，能够在 HTTP 客户端(Client)一侧存储并返回信息。HTTP 协议是一种无状态(Stateless)协议，Cookies 主要是对这一特性的补偿。这种简单的、持续的、客户端的状态，对基于 WWW 的应用程序(Application)的扩展产生了深远的影响。

下午科目答案与解析

试题一

答　案：

【问题 1】(1) Trunk　(2) VTP Server 或服务器模式　(3) VTP Client 或客户端模式　(4) VTP Transparent 或透明模式

注：(2)、(3)、(4)处答案次序任意。

(5) VTP 管理域

【问题 2】(6) 专线连接　(7) 分组交换

注：(6)、(7)处答案可以互换。

(8) 口令认证协议(Password Authentication Protocol，PAP)

(9) 质询握手认证协议(Challenge Handshake Authentication Protocol，CHAP)

注：(8)、(9)处答案可以互换。

【问题 3】(10) 生成树协议(Spanning Tree Protocol，STP)

【问题 4】(11) C 或虚拟专用网(VPN)技术　(12) D 或防火墙　(13) A 或 IP 地址绑定　(14) B 或数据库安全扫描

次建立连接时生成一个新的基本密钥，这些手段的采用使得诸如密钥共享、碰撞攻击和重放攻击等无能为力，从而弥补了 WEP 协议的安全隐患。

(67) 答　案：C。

解　析：无线路由器是具有路由功能的 AP，一般情况下，它不仅具备无线 AP 的所有功能，而且还包括了网络地址转换功能，因此可利用它建立一个更小范围的无线局域网，实现家庭无线网络中的 Internet 连接共享，实现 ADSL 和小区宽带接入。

(68) 答　案：C。

解　析：在进行网络设计时应充分考虑现有的网络结构，在不影响现有系统正常运行的情况下，逐步完善网络安全系统。

(69) 答　案：A。

解　析：不同的网络服务应用需要有不同的 QoS 要求。QoS 的关键指标包括可用性、吞吐量、时延、时延变化和丢失。ATM 的最大优势在于可以有效地实现 QoS。

(70) 答　案：A。

解　析：在网络分级设计模型中，核心层的主要功能是尽可能地进行数据交换。在核心层中不应该被牵扯到耗时的数据包操作或任何减慢数据交换的处理，因此，应该避免在核心层中使用访问控制列表或数据包过滤之类的功能，这一功能应由汇聚层来完成，答案选 A。

(71)～(75)答　案：(71)B；(72)C；(73)A；(74)D；(75)B。

参考译文：Cookies(小甜饼)最初由 Netscape Communications 提出，它是一种通用机制，这种机制使一个 HTTP 连接的服务端的应用程序，如 CGI、脚本(Script)，能够在 HTTP 客户端(Client)一侧存储并返回信息。HTTP 协议是一种无状态(Stateless)协议，Cookies 主要是对这一特性的补偿。这种简单的、持续的、客户端的状态，对基于 WWW 的应用程序(Application)的扩展产生了深远的影响。

下午科目答案与解析

试题一

答　案：

【问题 1】(1) Trunk　(2) VTP Server 或服务器模式　(3) VTP Client 或客户端模式　(4) VTP Transparent 或透明模式

注：(2)、(3)、(4)处答案次序任意。

(5) VTP 管理域

【问题 2】(6) 专线连接　(7) 分组交换

注：(6)、(7)处答案可以互换。

(8) 口令认证协议(Password Authentication Protocol，PAP)

(9) 质询握手认证协议(Challenge Handshake Authentication Protocol，CHAP)

注：(8)、(9)处答案可以互换。

【问题 3】(10) 生成树协议(Spanning Tree Protocol，STP)

【问题 4】(11) C 或虚拟专用网(VPN)技术　(12) D 或防火墙　(13) A 或 IP 地址绑定　(14) B 或数据库安全扫描



解　析：

【问题 1】

VTP(VLAN Trunk Protocol，VLAN 干道协议)的功能与 GVRP 相似，也是用来使 VLAN 配置信息在交换网内其他交换机上进行动态注册的一种二层协议。在一台 VTP Server 上配置一个新的 VLAN 信息，则该信息将自动传播到本域内的所有交换机上，从而减少在多台设备上配置同一信息的工作量，并且方便了管理。VTP 信息只能在 Trunk 端口上传播。

任何一台运行 VTP 的交换机可以工作在以下 3 种模式：VTP Server、VTP Client 及 VTP Transparent。

(1) VTP Server 维护该 VTP 域中所有 VLAN 信息列表，可以增加、删除或修改 VLAN。

(2) VTP Client 也维护该 VTP 域中所有 VLAN 信息列表，但不能增加、删除或修改 VLAN，任何变化的信息必须从 VTP Server 发布的通告报文中接收。

(3) VTP Transparent 不参与 VTP 工作，它虽然忽略所有接收到的 VTP 信息，但能够将接收到的 VTP 报文转发出去，它只拥有本设备上的 VLAN 信息。

交换 VTP 更新信息的所有交换机必须配置为相同的管理域。如果所有的交换机都以中断线相连，那么只要在核心交换机上配置一个管理域，网络上所有的交换机都将加入该域，这样管理域中所有的交换机都能够了解彼此的 VLAN 列表。

【问题 2】

远程访问是园区网络必须提供的服务之一，它可以为家庭办公用户和出差在外的员工提供移动接入服务。远程访问有 3 种可选的服务类型：专线连接、电路交换和包交换。异步拨号连接属于电路交换类型的广域网连接，它是在传统公共交换电话网上提供服务的，是最为方便和普遍的远程访问类型。

广域网连接可以采用不同类型的封装协议，如 HDLC、PPP 等。其中，PPP 除了提供身份认证功能外，还可以提供其他很多可选项配置，包括链路压缩、多链路捆绑和回叫等，因此更具优势。PPP 提供了两种可选的身份认证方法：口令认证协议(Password Authentication Protocol，PAP)和质询握手协议(Challenge Handshake Authentication Protocol，CHAP)。

【问题 3】

生成树协议(Spanning Tree)定义在 IEEE 802.1d 中，是一种链路管理协议，它为网络提供路径冗余的同时防止产生环路。为使以太网更好地工作，两个工作站之间只能有一条活动路径。

【问题 4】

在网络安全方面，可以采用分层控制方案，将整个网络分为外部网络传输控制层、内外网间访问控制层、内部网络访问控制层、操作系统及应用软件层和数据存储层，进而对各层的安全采取不同的技术措施。

外部网络是指局域网路由器和防火墙之外的公用网。当前网络技术发展迅速，因特网四通八达，网上黑客手段多种多样，为了保证安全，可以从以下方面采取措施：虚拟专网(VPN)技术、身份认证技术、加密技术、物理隔离等。

在内部局域网和外部局域网之间，可以采用以下技术来对外部和内部网络间的访问进行控制：防火墙、防毒网关、网络地址转换技术、代理服务及路由器、入侵检测等。

在局域网内部，非法用户的登录和对数据的非法修改更加不易查出。当用户安全意识

差、口令选择或保存不慎、账号转借和共享都会对网络安全造成极大的威胁，从内部网访问控制层进行安全防护，可采取以下措施：用户的身份认证、权限控制、加密技术、客户端安全防护等。

数据存储在服务器或加密终端上，数据存储的安全性是系统安全的重要组成部分。对数据的安全保护措施可以采用以下几种方式：使用较安全的数据库系统、加密技术、数据库安全扫描、存储介质的安全等。

试题二

答　案：

【问题1】(1) 61.246.100.96　(2) 61.246.100.103　(3) 5

【问题2】(4) 路由器禁止HTTP服务　(5) 配置路由器读写团体字符串为admin　(6) 设置ACL允许192.168.5.1访问CON 0

【问题3】(7) 255.255.255.248　(8) 192.168.50.0　(9) 0.0.0.255

解　析：该题考查的是DDN接入方式下路由器的配置。

本题第一问给定了一个公网IP及其子网掩码，要求本地路由出口上可用的公网IP地址范围及可用个数，只需计算出该网段类的IP地址个数(除去广播地址与网络地址外)，再减去一个对端所使用的IP即可。另外分别考查了启用路由器HTTP访问、设置团体口令，以及访问控制列表的配置命令。

【问题1】

根据题目提示，该单位申请的公网IP地址为61.246.100.96/29，因此该单位可用的IP地址范围是61.246.100.96～61.246.100.103。在这些地址中，广播地址、两个互连的路由器使用的接口地址不可用，因此可用地址为5个。

【问题2】参见路由器的配置部分。

【问题3】参见路由器的配置部分。

试题三

答　案：

【问题1】(1) 192.168.1.0　(2) 192.168.1.127　(3) 192.168.1.128　(4) 192.168.1.255　(5) 126

【问题2】(6) A或yes　(7) 255.255.255.128　(8) 255.255.255.128

【问题3】(9) ifup　(10) 网络接口(或设备)名称(或eth0或eth1)

【问题4】(11) eth0　(12) eth1

【问题5】(13) A或traceroute　(14) B或0

解　析：

【问题1】

本题中图示的网络由一台双网卡的网关计算机均分成两个子网，分别属于销售部和技术部，同部门的网络通信分别在各自的子网中进行，不同部门用户间的通信将由网关计算机进行转发，这样不再是所有的用户都在一个相同的、大型的网络上，子网划分的结果是提高了网络的速度。

整个网络的网络号是192.168.1.0，是一个C类网络，子网掩码是11111111.11111111.11111111.00000000(十进制表示为255.255.255.0)，即网络地址的前3个字节的每一位设置为

1，剩余的(主机地址)位设置为 0。当把剩余的表示主机地址的字节最高位设置为 1 时，网络就被均分成了两个子网，此时子网掩码为 11111111.11111111.11111111.10000000，用十进制表示为 255.255.255.128。

子网网络号可以用子网 IP 地址与子网掩码进行逐位 AND 运算得到。

销售部子网号：192.168.1.1(或 192.168.1.126)AND255.255.255.128 等于 192.168.1.0；

技术部子网号：192.168.1.129(或 192.168.1.254)AND255.255.255.128 等于 192.168.1.128。

对于销售部子网而言，主机号是 0 的地址(192.168.1.0)是子网掩码，不能分配给主机，主机位全为 1 的地址(192.168.1.127)是子网广播地址，保留，也不能分配给主机；对于技术部子网而言，主机号是 0 的地址(192.168.1.128)是子网掩码，不能分配给主机，主机位全为 1 的地址(192.168.1.255)是子网广播地址，保留，也不能分配给主机。因此这两个子网的可用 IP 地址是 126 个(128 减去 2 个保留地址)。

【问题 2】

Linux 计算机中，/etc/sysconfig/network 可配置文件定义了该计算机网络的基本属性，包括网络是否可用、是否允许 IP 包转发、主机域名、网关地址、网关设备名等。由于这台 Linux 计算机用于整个网络系统的网关，两个子网间的 IP 通信需要该计算机进行转发，因此文件中的 FORWARD_IPV4 应设置为“yes”，就本题而言，即支持 IP 包在两个网卡设备间转发。如果要将 IP 包转发关闭，则 FORWARD_IPV4 应设置为“no”。

网络接口文件/etc/sysconfig/network-scripts/ifcfg-eth0 定义了网络设备 eth0 的属性，由题目图示可知，该网络设备属于销售部子网，子网掩码为 255.255.255.128，即文件中的 NETMASK 应设置为“255.255.255.128”；同样网络接口文件/etc/sysconfig/network-scripts/ifcfg-eth1 中的 NETMASK 应设置为“255.255.255.128”。

【问题 3】

在/etc/sysconfig/network-scripts/目录中有许多脚本文件应用于基本网络管理，包括启动网络设备、停止网络设备运行等。常用的两个脚本命令是 ifup 和 ifdown，前者是启动网络设备运行，后者是停止网络设备运行，脚本以设备名为参数，设备名为 eth0、eth1 等。

【问题 4】

当正确地配置了/etc/sysconfig/network 文件、/etc/sysconfig/network-scripts/ifcfg-eth0 文件和/etc/sysconfig/network-scripts/ifcfg-eth1 文件，并成功运行 ifup 脚本命令启动了 eth0 设备和 eth1 设备后，还需要在网关计算机上使用 route 命令分别为两个子网创建两个默认路由。

route add -net 192.168.1.0 255.255.255.128 eth0，销售部子网通过 eth0 转发；

route add -net 192.168.1.128 255.255.255.128 eth1，技术部子网通过 eth1 转发。

上面的路由命令确保把指定的网络传输的数据包通过指定的接口设备进行传输。

【问题 5】

两个子网间的主机要能够正常通信，首先应该正确设置技术部和销售部的主机网络参数，比如销售部的主机的网关地址应设置为 192.168.1.126，技术部的主机的网关地址应设置为 192.168.1.254。进行连通性测试常用的命令是 ping，当发现两个子网间的主机 ping 失败时，可以在网关计算机上使用 traceroute 命令来确定数据包是否能够达到网关的另一端。如果 traceroute 显示数据可以到达网关但是不能转发到目标计算机上，问题就出在网关上。应该保证 IP 转发在网关计算机上是允许的，在网关计算机上运行 cat/proc/sys/net/ipv4/ip_forward，

查询内核的 IP 转发参数，如果返回的是 0，说明 IP 转发在内核中是禁止的，此时需要重新编译内核，使内核支持 IP 转发，即 cat/proc/sys/net/ipv4/ip_forward 的返回为 1。

试题四

答　案：

【问题 1】(1) A　(2) C

【问题 2】(3) 202.161.158.240 至 202.161.158.254 均可　(4) 255.255.255.240
(5) 202.161.158.239

【问题 3】(6) A　(7) H　(8) G　(9) E

【问题 4】(10) EBDCA

【问题 5】(11) B

【问题 6】(12) https://www.abc.com　(13) 443

解　析：

【问题 1】

为了确保 IIS 服务的安全，一个重要的前提就是让它安装在安全的系统上。在 Windows 服务器上安装 IIS 最好选用 NTFS 分区格式。因为在 NTFS 格式下，可以针对某个文件或文件夹给不同的用户分配不同的权限，并且可以使用系统自带的加密文件系统 EFS 对文件夹或文件进行加密。

【问题 2】

在 IIS 中，如果发现来自某一 IP 的计算机总是试图攻击网站，就可以使用“IP 地址及域名限制”来禁止其访问。通过 IP 地址及其域名限制，用户可以禁止某些特定的计算机或某个地址段中的计算机对子集的 Web 和 FTP 站点的访问。当有大量的攻击和破坏来自某些地址或某个子网时，使用这种限制机制是非常有用的。

为了禁止 IP 地址为 202.161.158.239～202.161.158.254 的主机访问该网站，可以将这个地址段中的所有 IP 地址以单个主机的形式加入限制访问的地址列表中，也可以 IP 地址加子网掩码的形式添加一组主机地址。这里如果采用子网掩码，那么 202.161.158.239 不在该网段，还需要单独添加该主机 IP。

【问题 3】

本题考查的是 SSL 安全加密机制的基础知识。SSL 是一个协议独立的加密方案，在网络信息包的应用层和传输层之间提供了安全的通道。

【问题 4】

IIS 使用的是 HTTP 协议，以明文的形式传输数据，没有采用任何加密手段，传输的重要数据容易被窃取。如果建立了 SSL 安全机制，只有 SSL 允许的客户才能与 SSL 允许的 Web 站点进行通信。

在 Windows Server 2003 中，为 IIS 安装 SSL 安全加密体制需要执行以下步骤。

(1) 生成证书请求文件。

(2) 安装证书服务。

(3) 申请 IIS 网站证书。

(4) 颁发 IIS 网站证书。

(5) 导入 IIS 网站证书。



(6) 配置 IIS 安全通信。

【问题 5】

导入证书后，IIS 并没有启用 SSL 安全加密功能，需要进一步对 IIS 服务器进行配置。在“目录安全性”选项卡中单击“安全通信”中的“编辑”按钮，弹出“安全通信”对话框，从中选择“要求安全通道(SSL)”和“要求 128 位加密”选项。接着单击“身份验证和访问控制”中的“编辑”按钮，弹出“身份验证方法”对话框，取消选中“启用匿名访问”和“集成 Windows 身份验证”复选框，只选中“基本身份验证”复选框即可。

【问题 6】

使用安装 SSL 安全加密机制的 Web 站点，需要在使用 URL 资源定位器时输入 https://。

试题五

答　案：

【问题 1】隧道技术、加解密技术、密钥管理技术、使用者与设备身份认证技术

【问题 2】(1) 配置 telnet 口令为 goodbad　(2) 设置串口 serial0/0 的数据封装形式为 PPP　(3) 在串口 serial0/0 中禁用 CDP

【问题 3】(4) ip nat inside　(5) ip nat outside

【问题 4】(6) 配置 AH 的哈希散列算法为 MD5　(7) 配置 IKE 策略性 10 的认证方法为预共享密钥

解　析：

【问题 1】

目前 VPN 主要采用 4 项技术来保证数据传输的安全性。一是隧道技术(Tunneling)，它是 VPN 的基本技术，类似于点对点连接技术，它在公用网上建立一条专用数据通道(隧道)，让数据包通过这条隧道传输；二是加解密技术(Encryption & Decryption)，VPN 可直接利用现有数据通信中较成熟的加解密技术；三是密钥管理技术(Key Management)，该技术的主要任务是保证如何在公用数据网上安全地传递密钥而不被窃取；四是使用者与设备身份认证技术(Authentication)，最常用的是使用者名称与密码或卡片式认证等方式。

【问题 2】

空(1)的上一条命令是进入虚拟终端 0～4 的线路(Line)配置模式，这条命令的作用是为配置 telnet 口令。空(2)是设置串口 serial0/0 的数据封装形式为 PPP。空(3)所在命令是在串口 serial0/0 关闭该功能。

【问题 3】

从网络结构和实现应用角度看，其目的是在路由器中实现 NAT 地址转换，将 ethernet0/0 端口指定为 NAT 转换内部网络接口，将 serial0/0 端口指定为 NAT 转换外部网络。在端口设置状态下，指定与内部网络相连的内部端口命令为 ip nat inside；指定与外部网络相连的外部端口命令为 ip nat outside。因此，空(5)和空(6)分别填“ip nat inside”和“ip nat outside”。

【问题 4】

空(6)处所在命令的作用是为 AH 选择哈希散列算法为 MD5，空(7)处所在命令的作用是为 IKE 策略 10 选择认证方法，pre-share 表示配置预共享密钥。

参 考 文 献

[1] 特南鲍姆，韦瑟罗尔．计算机网络[M]．5 版. 严伟，潘爱民译．北京：清华大学出版社，2012．
[2] 谢希仁．计算机网络[M]．7 版. 北京：电子工业出版社，2017．
[3] 雷震甲．网络工程师教程[M]．5 版. 北京：清华大学出版社，2018．
[4] 王达．华为交换机学习指南[M]．北京：人民邮电出版社，2013．
[5] 刘永华，孟凡楼等．Windows Server 2008 网络操作系统[M]．北京：清华大学出版社，2017．